PROFESSIONAL PROGRAMME

GROUP 1
ELECTIVE PAPER 4.2

INTERNAL & FORENSIC AUDIT

PART I – INTERNAL AUDIT

PART II – FORENSIC AUDIT

THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

STUDY MATERIAL

PROFESSIONAL PROGRAMME

INTERNAL & FORENSIC AUDIT

GROUP 1

ELECTIVE PAPER 4.2

THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

Timing of Headquarters :

Monday to Friday
Office Timings : 9.00 A.M. to 5.30 P.M.

Public Dealing Timings :

Without financial transactions – 9.30 A.M. to 5.00 P.M.
With financial transactions – 9.30 A.M. to 4.00 P.M.

Phones :

011-45341000 / 0120-4522000

Website :

www.icsi.edu

E-mail :

info@icsi.edu / academics@icsi.edu

For any suggestions/clarifications students may write to *academics@icsi.edu*

Laser Typesetting by :
AArushi Graphics, Prashant Vihar, New Delhi

PROFESSIONAL PROGRAMME

INTERNAL & FORENSIC AUDIT

India is leading its way towards attainment, progress and growth with global recognition as one of the fastest growing economies of the contemporary world. This emerging face of India is indeed a capture of spirited government's reform and initiatives under the realm of Good Governance.

The contemporary lead of good governance, which revolves around five 'E's being '*Effective, Efficient, Easy, Empower, and Equity'* calls for an accountable, transparent and developed face of a globally recognized welfare state.

In this direction, we are adopting a highly collaborative approach and addressing challenges like fraud, deceit, financial misplacement and alike, which are hindering the inclusive growth of India. Inter-alia, where fraud is considered as one of the critical ailments, which not only holdup the corporate organizations where it has been conducted, rather it shakes the entire economy sometimes with temporary effects and sometimes with permanent ones, it has always been the priority of growing economies including India to detect, prevent and regulate the menace of fraud in the larger interest of the nation.

In this selection of timely detection, prevention and regulation over corporate fraud and reference to due investigation, Internal & Forensic Audit is having an imperative role in assisting the corporates for maintaining efficiency and merit. On the larger parameters, Internal & Forensic audit as tool-mix of accounting and investigation is serving all the five E's of good governance and make the corporates to grow and develop on the parameters of being *Effective, Efficient, Easy, Empower, and Equity'*

In this background, where Internal & forensic audit is considered as a need of the hour for enhancing the corporate culture of India, varied roles are played by the Company Secretaries in the field of Internal & Forensic Audit. Further, the present day progressive changes in the Internal & Forensic Audit are expanding the gateway of opportunities for the professionals to guide, advice, operationalize, and appear in the matters related to Internal & Forensic Audit.

The Institute of Company Secretaries of India (ICSI), while persistently playing a pivotal role in building capacities of its members has decided to provide a 360 degree rounded set of learning to the students along with apprising them with the advanced changes in the arena of Internal & Forensic Audit and their directed implementation.

Therefore, this study material has been prepared to provide the students with a wide perspective and in-depth knowledge in Internal & forensic audit to enable them to get solid grounding in the legislative framework, practice and procedure of the Internal & forensic audit. The course contents of this study material have been so designed as to develop specialised skills in the corpus and complexities of the different aspects of the subject besides meeting the requirements of a future career in this area.

The Study Material which is divided in two parts covers in the details the concepts of Internal Audit in Part – I and discusses Forensic Audit in detail under Part-II.

The domain of Internal & forensic audit is vast. Every effort has been made to provide a self- contained material and an integrated approach has been adopted throughout.

The legislative changes made upto May 31, 2023 have been incorporated in the study material. In addition to Study Material students are advised to refer to the updations at the Regulator's website, supplements relevant for the subject issued by ICSI and ICSI Journal Chartered Secretary and other publications. Specifically, **students are advised to read "Student Company Secretary" e-Journal which covers regulatory and other relevant developments relating to the subject,** which is available at academic portal *https://www.icsi.edu/student-n/academic-portal/*. In the event of any doubt, students may contact the Directorate of Academics at academics@icsi.edu.

The amendments to law made upto 31st May of the Calendar Year for December Examinations and upto 30th November of the previous Calendar Year for June Examinations shall be applicable.

Although due care has been taken in publishing this study material, the possibility of errors, missions and /or discrepancies cannot be rules out. This publication is released with an understanding that the Institute shall not be responsible for any errors, omissions and/or discrepancies or any action taken in that behalf.

PROFESSIONAL PROGRAMME

Group 1

Elective Paper 4.2

INTERNAL & FORENSIC AUDIT

SYLLABUS

OBJECTIVES

Part I: To provide skills and knowledge required to conduct Internal Audit and open new vistas of opportunities for Company Secretaries in the field of internal auditing as well as to add tangible value to their organisations.

Part II: To understand and analyse the concept of Corporate Fraud and Forensics Auditing in the contemporary world along with the legal mechanism to counter the corporate fraud and understanding Forensic Audit and its methods.

Level of Knowledge : Expert Knowledge

Part I : Internal Audit (60 Marks)

1. **Internal Audit: Introduction & Overview:** Definition, Key Concept, Purpose, Authority and Responsibility of Internal Auditing ● Internal Auditor vs. External Auditor ● Types of Internal Audit ● Qualification and Appointment of Internal Auditor ● Strategic and Operational Role of Internal Auditor
2. **Practices related to Internal Auditing:** Laws, Standards and Regulations on Internal Auditing - National and International ● Internal Auditing Practices ● Corporate / Organizational Governance Principles ● Code of Ethics
3. **Internal Controls:** Meaning and Definition of Internal Control ● Dimensions of Internal Control ● Types of Controls (Preventive, detective, input, output) ● Internal Control Techniques ● Internal Control Frameworks (COSO, Cadbury) ● Role of Internal Auditors in Implementation of Internal Controls ● Examine the effectiveness and efficiency of internal controls ● Fraud Risk Awareness ● Risk Management ● Recommend controls to prevent and detect fraud and educate to improve the organization's fraud awareness
4. **Internal Audit Engagements and Planning :** Plan Engagements ● Supervise Engagement ● Communicate Engagement Results ● Monitor Engagement Outcomes ● Audit Planning and Stages for Internal Audit Planning
5. **Internal Audit Tools and Techniques**: Data Gathering ● Data Analysis, Interpretation and Reporting ● Documentation / Work Papers ● Process Mapping including Flowcharting ● Steps in evaluation and its techniques ● Use of Sampling Techniques and its tests ● Flowcharts and Internal Control Questionnaires ● Automation
6. **Internal Audit of Specific Functions:** Internal Audit of Purchase & Inventory Management ● Internal Audit of Production and Operations ● Internal Audit of Finance and Accounts ● Internal Audit of Human Resources ● Internal Audit of Sales & Marketing ● IT System Audit

7 **Special Points relating to Internal Audit in various entities:** Banking Companies ● Insurance Companies ● Cooperative Societies ● Public Sector Undertakings ● Partnership ● Shipping Companies ● Electric Supply Company ● Hotels ● Hospital ● Others

8. **Reporting under Internal Audit:** Observation Formulation ● Report Writing ● Monitoring Closure of Issues ● CARO - Companies (Auditors Report) Order

9. **Emerging Issues and Challenges:** Financial Accounting and Funding Risks ● Business related Challenges ● Project Management/Organizational Change ● In-house vs. Outsourcing Audit Assignments ● Emerging Issues

Part II : Forensic Audit (40 Marks)

10. **Basic Concepts of Forensic Audit:** Introduction ● Need and Objectives of Forensic Audit ● Fundamentals of Forensic Audit ● What is Fraud ● Kinds of Frauds ● Forensic Audit vis-a-vis Audit ● Modern Day Scenario

11. **Audit and Investigations:** Tools for handling Forensic Audit ● Investigation Mechanism ● Field Investigations ● Methods of Investigations ● Red Flags ● Green Flags ● Financial Statement Analysis

12. **Forensic Audit: Laws and Regulations:** Information Technology and Business Laws ● International Laws and Practices ● UK Bribery Act ● US Foreign Corrupt Practices Act ● Indian Laws ● ICSI Anti Bribery Code

13. **Forensic Audit and Indian Evidence Law:** Finding Facts ● Relevant Facts ● Admission of Evidence ● Methods to Prove Cases

14. **Cyber Forensics:** Introduction to Cyber Crime ● International Guidance to Cyber Forensics Laws ● Digital Forensics and Cyber Laws ● Introduction to Data Extraction ● Digital Forensics and Cyber Crime ● Ethical Hacking ● Digital Incident Response ● Case Laws: Indian and International

15. **Fraud Detecting Techniques:** Early Warning Indicators of fraud, Money laundering, misconduct ● General Audit Techniques ● Statistical & Mathematical Techniques ● Technology Based/ Digital Forensics Techniques ● Data mining techniques ● Willful defaults and Corporate Insolvency & Bankruptcy – emerging Forensic audit aspects

ARRANGEMENT OF STUDY LESSONS
INTERNAL & FORENSIC AUDIT
GROUP 1 • ELECTIVE PAPER 4.2

PART I: INTERNAL AUDIT

PART II: FORENSIC AUDIT

LESSON WISE SUMMARY
INTERNAL & FORENSIC AUDIT

PART I – INTERNAL AUDIT (60 MARKS)

Lesson 1 – Internal Audit: Introduction & Overview

Audit is the systematic scrutiny of books of accounts of an organization in order to calculate, ascertain or check their accuracy and efficiency. In the same line, Internal Audit is the check to assess the risk management and to ensure that risk management processes are efficient, effective, secure and compliant. It is the basic check of internal control of the organization. An internal audit is an organizational move to check, ensure, monitor and analyze its own business operations in order to determine how well it conforms to a set of specific criteria. The coverage of the lesson includes:

- The concept of Internal Audit and the regulatory provision mandatorily required to conduct Internal Audit
- The purpose or objectives for conducting Internal Audit
- The Role and Responsibilities of Internal Auditor
- The difference between Internal Audit and Statutory Audit
- The various types of Internal Audit such as Operational Audit, Compliance Audit, Environmental Audit, Performance Audit, Special Audit, Information System Audit
- The basics skills required to perform Internal Audit

Lesson 2 – Practices related to Internal Auditing

In this lesson, we will strive to understand the relevant regulations, applicable standards and generally accepted practices in the internal audit activity of an organisation. The coverage of the lesson includes:

- Several laws and regulations such as Companies Act, 2013, SEBI, RBI, IRDAI govern internal audit in India
- The laws of foreign government or regulators governing internal audit
- Section 138 of Companies Act, 2013 read along with Rule, 2014 impacting internal audit
- Standards on Internal Audit 'SIA' in India
- International Standard issued by Institute of Internal Auditor 'IIA'

Lesson 3 – Internal Controls

Internal controls are the mechanisms, rules and procedures implemented by an entity to ensure the integrity and reliability of financial and non-financial records, management information and cost accounting records, promote accountability, prevent and detect errors and frauds. The auditors also rely on the system of internal control for the purpose of audit of the financial accounts.

Internal control comprise internal accounting controls and operational controls. The auditors are primarily concerned with internal accounting controls.

Basic controls include features like control accounts and numerical controls to ensure that all transactions are completely accounted for in the books of account. Disciplines over basic controls include the segregation of incompatible duties, segregation of custody of assets from the accounting responsibilities, physical safeguards to prevent unauthorised access to assets or accounting and other sensitive records and internal check. The coverage of the lesson includes:

- Role of internal auditors in implementation of internal controls
- Examine the effectiveness and efficiency of internal controls
- Fraud risk awareness, Risk Management, Types of Risks, Enterprise Risk Management, Risk Management Plan
- Recommend internal controls to prevent and detect fraud and educate to improve the organisation's fraud awareness
- The role of Internal Control in the New Digital ERA such as Robotic Process Automation (RPA), Artificial Intelligence and Machine Learning, Block chain Technologies, Cloud Computing

Lesson 4 – Internal Audit Engagements and Planning

In the case of Companies under Companies Act, 2013, it is a legal requirement for the Audit Committee or its Board of Directors to formulate the overall internal audit plan of the company. Companies (Accounts) Rule 13(2) of Companies Act, 2013 provides: "The Audit Committee of the company or the Board shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity, and methodology for conducting the internal audit."

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the Institute of Chartered Accountants of India (ICAI), The Audit Committee or the Board takes the active support of the Chief Internal Auditor, to develop the Overall Internal Audit Plan, in consultation with the Executive Management.

The coverage of the lesson includes:

- Audit Plan and how to develop the Audit Plan
- The steps involved in Audit Planning
- Benefits for formulating Audit Plan
- Audit Universe and Factors for developing Internal audit universe
- Supervise Audit Engagement and monitor Audit Engagement Outcomes

Lesson 5 – Internal Audit Tools and Techniques

The coverage of the lesson includes:

- The concepts of documentation, nature and purpose of documentation, Important aspects in Documentation, Form, content and extent of documentation, audit file, Type of File , Permanent File, Current File
- The need for working papers, ownership and custody of working papers, Guidelines for preparation of working papers, Documents Checklist
- Audit evidence, Sources of Audit evidence, sufficiency and appropriateness of audit evidence, types of audit evidence, relevance and reliability of audit evidence. The Importance of written representations and the objectives, External Confirmation and its relevance

- Internal Audit Techniques such as Vouching, Inquiry and Confirmation, Reconciliation, Testing, Physical Verification, Analytical Procedure, Computation, Flowchart, Observation
- Audit Sampling, Application of Audit Sampling Techniques, Sample Selection Methods, Sampling Risk, Evaluating Results of Audit Sampling
- Flowchart and Internal Control Questionnaire, Audit in Automation Environment

Lesson 6 – Internal Audit of Specific Functions

In the previous lesson, we have studied about internal audit tools and techniques, and how they can be used effectively while conducting an internal audit. In this lesson we take the discussion forward and learn about nuances of conducting internal audit of some specific functions or processes which are usually part of most of the organisations. We will strive to understand the practical aspects as well the possible risks and controls which may be audited in such audits. The coverage of the lesson includes:

A. Internal Audit of Purchasing Activity

B. Internal Audit of Inventory Management

C. Internal Audit of Production and Operations

D. Internal Audit of Finance and Accounts

E. Internal Audit of Human Resources

F. Internal Audit of Sales & Marketing

G. IT System Audit

Lesson 7 – Special Points relating to Internal Audit in various entities

The coverage of the lesson includes the Major's points / areas to be covered in case of audit of Banking Companies, Insurance Companies, Cooperative Societies, Public Sector Undertakings, Partnership, Shipping Companies, Electric Supply Company, Hotels, and Hospital etc.

Lesson 8 – Reporting under Internal Audit

The essential part of internal audit is the dissemination of the results of internal audit and reports the findings to management, and those charged with governance. The internal audit report of the company is a significant aspect which throws light on any kind of non-compliance with the regulations that are needed to be kept in mind. It also highlights the aspects which need to be improved.

The internal auditor should review and assess the analysis drawn from the internal audit evidence obtained as the basis for his conclusion on the efficiency and effectiveness of systems, processes and controls including items of financial statements.

The coverage of the lesson includes:

- The reporting under Internal Audit and objectives of Reporting under Internal Audit
- Important aspects of quality reporting under Internal Audit
- Layout of Internal Audit Report
- The precautions to be taken care of while drafting Internal Audit Report?
- Communication of outcomes of Internal Audit to Management

- Checklist of Internal Audit Report
- Reporting under various clauses of Companies Audit Report Order 2020 [CARO 2020]

Lesson 9 – Emerging Issues and Challenges

Many businesses have to take risks when it comes to their finances. Whether it's investing in new projects or increasing production, there is always the potential for failure. But with the proper financial accounting and funding risk management techniques, one can minimise their risk and ensure the success of business. Financial accounting and funding risk are two different topics, but they go hand in hand. Financial accounting is the process of recording and summarising financial information, while funding risk is the potential for losses due to inadequate or inappropriate funding. How financial accounts are managed can significantly influence the level of funding risk a company faces.

Poorly managed accounts can lead to insufficient funds, which in turn, can lead to cash flow problems and other financial issues. On the other hand, well-managed accounts enable companies to utilise their resources efficiently and effectively, minimising their exposure to funding risks. Let's explore different ways to manage financial accounting and funding risks. We will also look at how financial accounting and funding risk are related and how organisations should manage their finances to reduce risk exposure.

The coverage of the lesson includes:

- Financial Accounting & the risks involved in Financial Accounting?
- Funding Risks and how it can be avoided?
- Various business related challenges while conducting internal audit
- Prons and Cons of In-house Internal Audit function and of Outsourcing of Internal Audit function
- Prons and Cons of Co-sourcing of audit assignment
- Various emerging areas to be looked in Internal Audit

PART II – FORENSIC AUDIT (40 MARKS)

Lesson 10 – Basic Concepts of Forensic Audit

In the selection of timely detection, prevention and regulation over corporate fraud and reference to due investigation, Forensic Audit is having an imperative role in assisting the corporates for maintaining efficiency and merit. On the larger parameters, Forensic audit as tool-mix of accounting and investigation is serving all the five E's of good governance and make the corporates to grow and develop on the parameters of being Effective, Efficient, Easy, Empower, and Equity'. In this background, where forensic audit is considered as a need of the hour for enhancing the corporate culture of India, this chapter covers the verve of the forensic audit including the meaning, definition, objectives and significance of forensic audit.

In the contemporary era, Government of India is adopting a highly collaborative approach and addressing various challenges like fraud, deceit, financial misplacement and alike, which are a big hindrances in the path of inclusive growth of corporates in India. Among other things, 'fraud' in one of the most critical ailments which not only holdups the corporate organizations where it is conducted, rather it shakes the economy of entire country which has both short term as well as long term impact. In this whole process of timely detection of frauds and reference of such case for due investigation, Forensic Audit has an imperative role in assisting the corporates to maintain efficiency as well as merit at par. In the larger perspective, this lesson aims to apprise the students with modern day scenario of forensic audit, fundamentals of forensic audit along with other related concepts.

Lesson 11 – Audit and Investigations

Right from conducting forensic audit to examining the evidences, from finding the culprit behind the fraud to appearing in the court for submitted the testimony, a Company Secretary is apt in serving his professional excellence as a forensic auditor.

To summarize, where forensic audit is a detailed engagement which requires the expertise of not only accounting and auditing procedures but also expert knowledge regarding the legal framework, and a forensic auditor is required to have an understanding of various frauds that can be carried out and of how evidence needs to be collected.

In this context, Company Secretary is a Catalyst in Upholding Good Governance via Forensic Audit. His role in specific to Forensic audit is the main objective of this lesson. Henceforth, the lesson aims to provide a clear understanding to the matters including Tools for handling Forensic Audit and the Role of Company Secretary; Investigation Mechanism; Field Investigations; Methods of Investigations; Red Flags; Green Flags and alike.

Lesson 12 – Forensic Audit: Laws and Regulations

A forensic audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in the court of law. A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims. In order to understand the legal consequences that a person attracts on being caught in a forensic audit, it is necessary to know about the various statutes that talk about the implementation of forensic audits in India. Therefore, this lesson aims at providing the basic understanding as to the laws, regulations and statues, nationally as well as internationally, dealing will corporate laws and empowering forensic auditors in performing their duties in its true letter and spirit.

Lesson 13 – Forensic Audit and Indian Evidence Law

In order to prove a case in the court of law and to penalize the wrong doers, the matter must be proved beyond reasonable doubt. For this purpose, one must adduce relevant evidences in the court of law. The similar context is applicable for proving the corporate fraud and the person behind it through the use of forensic audit reports. Therefore, this lesson deals with the concepts of evidence law in reference to forensic audit. In specific, it deals with Finding Facts; Relevant Facts; Admission of Evidence; Methods to Prove Cases.

Lesson 14 – Cyber Forensics

The impact of Information and Communication Technology is very profound. Both Society and the Technology are operating in a way so as to harmonize with the pace of each other's growth. As the World is developing, more technology is emerging with each passing day and thus there is more development taking place in the society. All the facets of human life including education, health, entertainment and communication are being influenced by and have been impacted by the advent of the Information and Communication Technology. This way, Information Technology is rightly called as a boon.

With boon goes the bane, so is the case with Information and Communication Technology. One of the major challenges in this era of ICT is of an increasing number of cyber-crimes taking place in the World today. Corporate Frauds are not the exception to it.

In the light of corporate frauds executed via the means of Information Technology, a new branch of forensic audit called Cyber Forensics audit has emerged in the contemporary world.

In this perspective, this chapter aims to apprise the students with concepts like Cyber Crime; International Guidance to Cyber Forensics Laws; Digital Forensics and Cyber Laws; Introduction to Data Extraction; Digital Forensics and Cyber Crime; Ethical Hacking, Digital Incident Response and alike.

Lesson 15 – Fraud Detecting Techniques

The coverage of the lesson includes:

- The meaning of Fraud, Investigation and Detection
- Early warning indicators of Fraud such as Unusual Financial Activity, Poor Accounting, Unusual behavior, Unexplained Inventory, Employee Turnover, Weak or lack of Internal Controls, Complaints or Tip, Weaknesses in IT Security, Suspicious Emails or Messages
- The term 'Money Laundering' and Techniques used for Fraud Detection in Money Laundering
- Fraud Detection using General Audit Techniques such as Analytical procedures, Inquiry, Observation, Re-performance, Sampling, Inspection etc.
- Statistical and Mathematical Techniques in Fraud Detection
- Technology based Fraud Detection Techniques
- Data Mining Techniques for Fraud Detection

CONTENTS

PART I – INTERNAL AUDIT

LESSON 1
INTERNAL AUDIT: INTRODUCTION & OVERVIEW

LESSON 2
PRACTICES RELATED TO INTERNAL AUDITING

LESSON 6

INTERNAL AUDIT OF SPECIFIC FUNCTIONS

LESSON 8

REPORTING UNDER INTERNAL AUDIT

LESSON 11

AUDIT AND INVESTIGATIONS

LESSON 12

FORENSIC AUDIT : LAWS AND REGULATIONS

LESSON 13

FORENSIC AUDIT AND INDIAN EVIDENCE LAW

LESSON 14

CYBER FORENSICS

LESSON 15

FRAUD DETECTING TECHNIQUES

PART I

INTERNAL AUDIT

Internal Audit: Introduction & Overview

Lesson 1

KEY CONCEPTS

■ Internal Audit ■ Statutory Audit ■ Operational Audit ■ Compliance Audit ■ Environmental Audit ■ Performance Audit ■ Special Audit ■ Information System Audit

Learning Objectives

To understand:

- The concept of Internal Audit
- The regulatory provision mandatorily required to conduct Internal Audit
- The purpose or objectives for conducting Internal Audit
- The Role and Responsibilities of Internal Auditor
- The difference between Internal Audit and Statutory Audit
- The various types of Internal Audit such as Operational Audit, Compliance Audit, Environmental Audit, Performance Audit, Special Audit, Information System Audit
- Who can be appointed as Internal Auditor?
- What are the basics skills required to perform Internal Audit?

Lesson Outline

- Introduction and Definition
- Applicability of the Provisions of Internal Audit
- Purpose of Internal Audit
- Objectives of Internal Audit
- Authority and Responsibilities of Internal Audit
- *Internal Auditor* vs. *External Auditor*
- Types of Internal Audit
- Qualification and Appointment of Internal Auditor
- Strategic and Operational Role of Internal Auditor
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION AND DEFINITION

Audit is the systematic scrutiny of books of accounts of an organization in order to calculate, ascertain or check their accuracy and efficiency. In the same line, Internal Audit is the check to assess the risk management and to ensure that risk management processes are efficient, effective, secure and compliant. It is the basic check of internal control of the organization. An internal audit is an organizational move to check, ensure, monitor and analyze its own business operations in order to determine how well it conforms to a set of specific criteria.

The internal auditing profession evolved steadily with the progress of management science after World War II. It is conceptually similar in many ways to financial auditing by public accounting firms, quality assurance and compliance activities. While some of the audit technique underlying internal auditing is derived from management consulting and public accounting professions, the theory of internal auditing was conceived primarily by Lawrence Sawyer, often referred to as "the father of modern internal auditing" and the current philosophy, theory and practice of modern internal auditing as defined by the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors owes much to Sawyer's vision.

In the past, internal auditing was constrained to ensure that, the accounting and allied records have been properly maintained, the assets of the organization have been properly safeguarded and that the policies and procedures laid down by the management have been complied with. Thereafter post liberalization of economy, the growth and expansion made it increasingly difficult for organizations to maintain control and operational efficiency. It was difficult for management to observe all the operating areas or be in touch with everybody. This requires companies or the entities to appoint auditing personnel for report on affairs of the company, which are known as 'Internal Auditors'.

Many modern enterprises have become huge and sophisticated. This has resulted in decentralisation of the activities and consequently, the top management is remotely concerned with the day-to-day activities of the concern. With the changes in the economic conditions, now the scope of internal auditing is not confined to financial transactions it is extended up to the minuet activity of the company, which may or may not be the cost center but have an impact on the efficiency on the company. Accordingly, in the present dynamic business model scenario, the role of internal auditing has a great significance in the performance of the company.

Internal audit is an evaluation and analysis of the business operation conducted by the internal audit staff. It is the part of evaluation of overall system of internal control established in an organization. Internal audit is the independent appraisal activity within an organization for the review of accounting, financial and other business practices as protective and constructive arms of management. It is a type of control which functions by measuring and evaluating the effectiveness of other type of controls.

Some of the definitions of Internal Auditing are appended below:

The Institute of Internal Auditors (IIA) defines Internal Audit as follows: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".

The Institute of Chartered Accountants of India (ICAI) defined Internal Audit as "an independent management function, which involves a continuous critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system".

According to Professor Walter B. Meigs, Internal Auditing means "Internal auditing consist of a continuous, critical review of financial and operating activities by a staff of auditors functioning as full time salaried employees."

In a big organization, an internal audit is carried out by the team of professionals in the organization. This provides management an assurance about the control process in the organization and it aids in early detection of inefficiencies/fraud etc. It helps the statutory auditor to conduct the statutory audit effectively.

APPLICABILITY OF THE PROVISIONS OF INTERNAL AUDIT

As per section 138 of the Companies Act, 2013, following class of companies [prescribed in rule 13 of Companies (Accounts) Rules, 2014] shall be required to appoint an internal auditor which may be either an individual or a partnership firm or a body corporate, namely-

(a) every listed public company;

(b) every unlisted public company having

(i) paid up share capital of fifty crore rupees or more during the preceding financial year; or

(ii) turnover of two hundred crore rupees or more during the preceding financial year; or

(iii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year; or

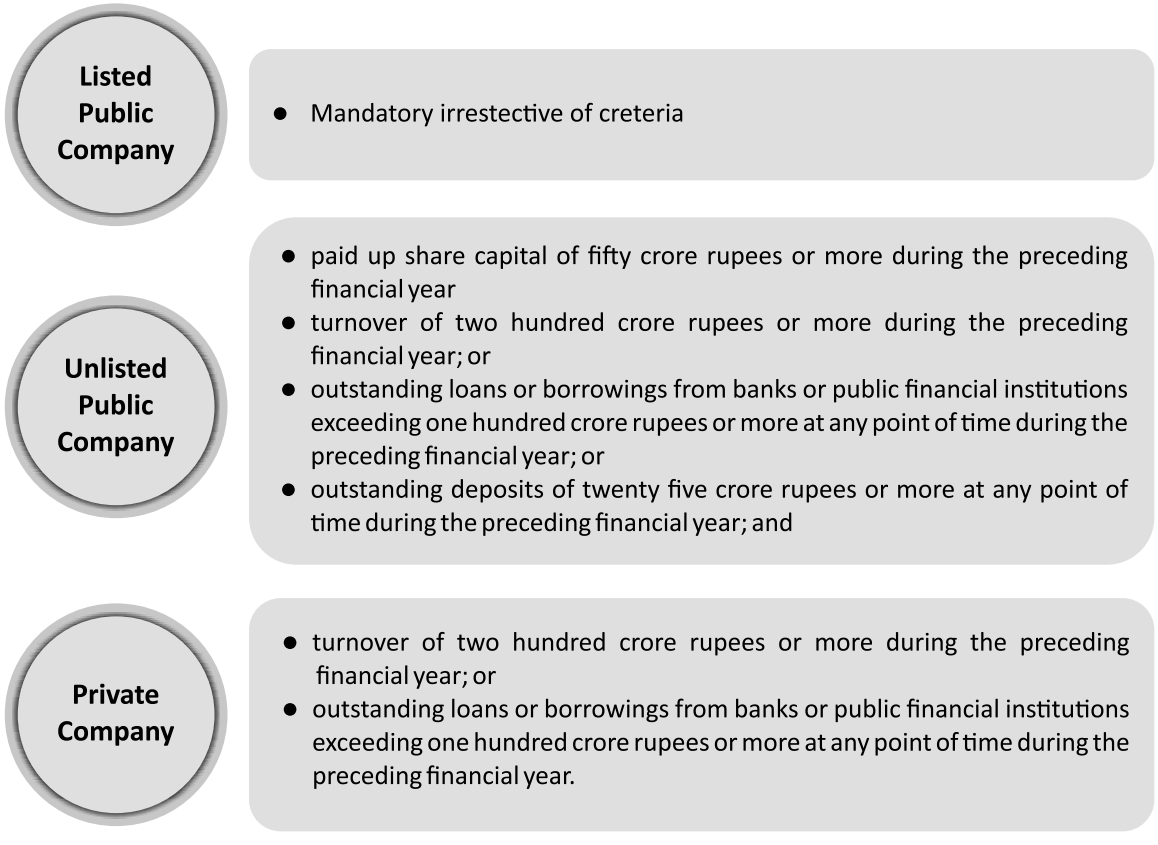
(iv) outstanding deposits of twenty five crore rupees or more at any point of time during the preceding financial year; and

(c) every private company having-

(i) turnover of two hundred crore rupees or more during the preceding financial year; or

(ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.

It is provided that when an existing company gets covered under any of the above criteria shall comply with the requirements within six months of commencement of such applicability.



Penalty for Non-Compliance

If a company or any other officer of the company, contravenes the provisions of this section, then the company or any officer of the company who is in default is liable for punishment with a penalty of up to Rs.10,000. In case of continuation of default in complying with the above section further fine of Rs.1,000 per day will be imposed subject to a maximum of Rs. 2,00,000 in case of a company and Rs. 50,000 in case of an officer who is in default or any other person.

CASE STUDY

1. ABC Pvt. Ltd. having Rs. 90 lacs paid-up capital, Rs. 5 crores reserves and turnover of last three consecutive financial years, immediately preceding the financial year under audit, being Rs. 50 crores, Rs. 175 crores and Rs. 300 crores, but does not have any internal audit system. In view of the management, the internal audit system is not mandatory. Comment?

Solution:

Applicability of Provisions of Internal Audit: As per section 138 of the Companies Act, 2013, read with rule 13 of Companies (Audit and Auditors) Rules, 2014, every private company shall be required to appoint an internal auditor or a firm of internal auditors, having-

(i) turnover of two hundred crore rupees or more during the preceding financial year; or

(ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.

Conclusion: In the instant case, ABC Pvt. Ltd. is having a turnover of Rs. 300 crores during the preceding financial year which is more than two hundred crore rupees. Hence, the company has the mandatorily statutory requirement to appoint an Internal Auditor and mandatorily conduct an internal audit.

2. Shree Solution Pvt. Ltd. having a negative net worth of Rs. 120 lacs. However, turnover of last financial years, immediately preceding the financial year under audit, being Rs. 150 crores. Further, borrowing loans from SBI limited were 150 crore on 1st April, 2021. During the FY 2021-22, company has repaid the loan in full. In view of the management, the internal audit system is not mandatory for FY 2022-23. Comment?

Solution:

Applicability of Provisions of Internal Audit: As per section 138 of the Companies Act, 2013, read with rule 13 of Companies (Audit and Auditors) Rules, 2014, every private company shall be required to appoint an internal auditor or a firm of internal auditors, having-

(i) turnover of two hundred crore rupees or more during the preceding financial year; or

(ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.

Conclusion: In the instant case, Shree solution Pvt. Ltd. is having a turnover of Rs. 150 crores during the preceding financial year which is less than two hundred crore rupees. However, the company has a outstanding loan of Rs. 150 crore on 1st April, 2021 i.e. during the any point of time in FY 2021-22 which is more than 100 crores.

Hence, the company has the mandatorily statutory requirement to appoint an Internal Auditor and mandatorily conduct an internal audit for FY 2022-23.

3. Aman Pvt. Ltd. (listed in NSE) having a turnover of last financial years, immediately preceding the financial year under audit, being Rs. 120 crores. Further, borrowing loans from SBI limited were 90 crore on 1st April, 2021. During the FY 2021-22, company has repaid the loan in full. In view of the management, the internal audit system is mandatory for FY 2022-23 as Aman Pvt. Ltd. is listed in NSE. Comment?

Solution:

Applicability of Provisions of Internal Audit: As per section 138 of the Companies Act, 2013, read with rule 13 of Companies (Audit and Auditors) Rules, 2014, every private company shall be required to appoint an internal auditor or a firm of internal auditors, having-

(i) turnover of two hundred crore rupees or more during the preceding financial year; or

(ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.

Conclusion: In the instant case, Aman Pvt. Ltd. is having a turnover of Rs. 120 crores during the preceding financial year which is less than two hundred crore rupees. Further, the company has an outstanding loan of Rs. 90 crore on 1st April, 2021 i.e. during the any point of time in FY 2021-22 which is less than 100 crores.

Hence, the company is not mandatorily statutory requirement to appoint an Internal Auditor irrespective of the fact that it is listed in NSE.

4. Will the Partnership firm / Proprietary firm mandatorily required appointing an Internal Auditor?

Solution:

No, the Partnership firm / Proprietary firm is not mandatorily required to appoint an Internal Auditor. However, voluntary the Partnership firm / Proprietary firm can appoint an internal auditor of the organization.

5. Is there any penalty for non-compliance with respect to appointment of internal auditor?

Solution:

Yes, If a company or any other officer of the company, contravenes the provisions of this section, then the company or any officer of the company who is in default is liable for punishment with a penalty of up to Rs.10,000. In case of continuation of default in complying with the above section further fine of Rs.1,000 per day will be imposed subject to a maximum of Rs. 2,00,000 in case of a company and Rs. 50,000 in case of an officer who is in default or any other person.

PURPOSE OF INTERNAL AUDIT

To verify the correctness, accuracy, and authenticity of the financial accounting and statistical records presented to the management.

To confirm that the organization has incurred liabilities concerning its valid and legitimate activities.

To comment on the effectiveness of the internal control system and the internal check system in force and to suggest ways and means to improve these systems.

To facilitate the early detection and prevention of fraud.

To examine the protection afforded to the company's assets and their use for business purposes.

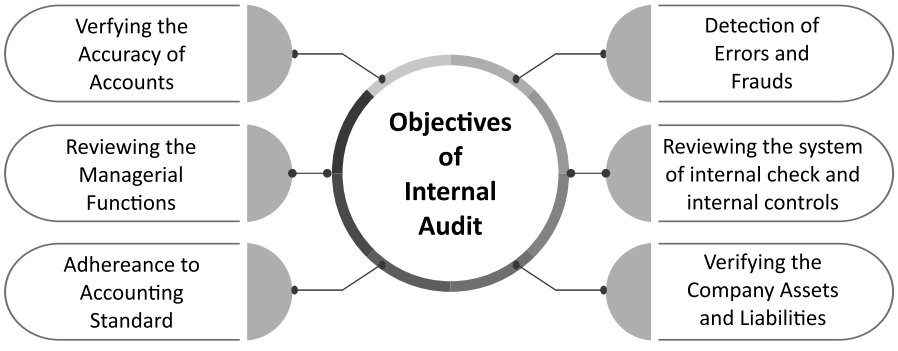
To identify the authorities responsible for purchasing assets and other items as well as disposal of assets.

To ensure that the standard accounting practices that the organization must follow are strictly followed.

To undertake a special investigation for the management.

To assist management in achieving the most efficient administration of the operation by establishing procedures by complying with the company's operating policies.

OBJECTIVES OF INTERNAL AUDIT



AUTHORITY AND RESPONSIBILITY OF INTERNAL AUDITING

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation in accomplishing its objectives by bringing a

systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

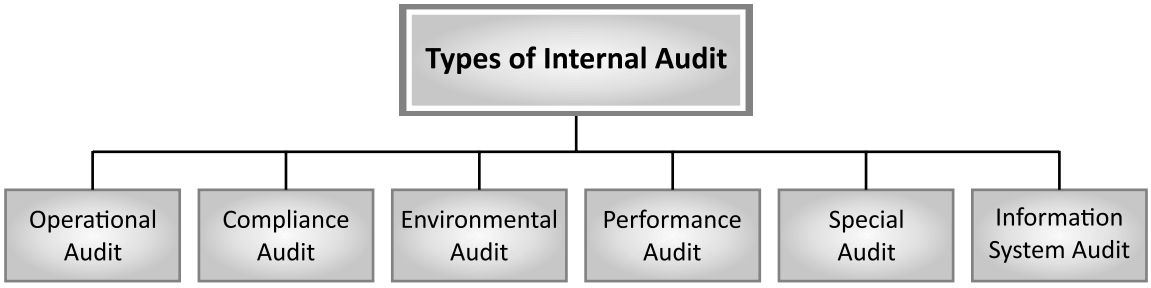
1. To work with board and management to ensure that a system is in place which ensures that all major risks are identified and analyzed. Evaluate and provide reasonable assurance that risk management, control, and governance systems are functioning as intended and will enable the organisation's objectives and goals to be met.
2. To plan, organize and carry out the internal audit function including the preparation of an audit plan which fulfils the responsibility of the department, scheduling and assigning work and estimating resource needs.
3. Report risk management issues and internal controls deficiencies identified directly to the audit committee and provide recommendations for improving the organization's operations, in terms of both efficient and effective performance.
4. Evaluation of information security and associated risk exposures. Evaluation of the organisation's readiness in case of business interruption.
5. Evaluation of regulatory compliance program with consultation from legal counsel.
6. Maintain open communication with management and the audit committee. Team with other internal and external resources as appropriate. Engage in continuous education and staff development. To report to both the audit committee and management on the policies, programmed and activities of the department.
7. Provide support to the company's anti-fraud programs.
8. To coordinate coverage with the external auditors and ensure that each party is not only aware of the other's work but also well briefed on areas of concern.
9. To make recommendations on the systems and procedures being reviewed, report on the findings and recommendations and monitor management's response and implementation.
10. To review and report on the accuracy, timeliness and relevance of the financial and other information that is provided for management.
11. To associate closely with management and keep knowledge up to date by being informed about all important occurrences and events affecting the business, as well as the changes that are made in business policies.

INTERNAL AUDITOR VS. EXTERNAL AUDITOR

Basis for Comparison	***Internal Audit***	***External Audit***
Meaning	It refers to an ongoing audit function performed within an organization by a separate internal auditing department.	It is an audit function performed by the independent body which is not a part of the organization.
Examination	Internal auditor examines the Operational efficiency of the organisation.	External auditor examines the Accuracy and Validity of Financial Statements.
Appointment	Internal auditor is appointed by the Management.	External auditor is appointed by the Members.

Users of Report	User of internal audit report is Management.	User of external audit report is Stakeholders.
Period	Internal audit is a Continuous Process throughout the year.	External audit is done once in a year.
Opinion	Opinion is provided on the effectiveness of the operational activities of the organization.	Opinion is provided on the truthfulness and fairness of the financial statement of the company.
Status of Auditor	Internal auditor could be an employee of the company, thus, less independent.	External auditor is an independent person and not an employee of the company.

TYPES OF INTERNAL AUDIT

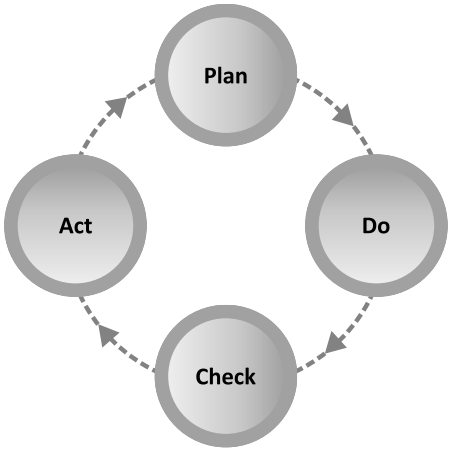


Operational Audit: Operational audit is an audit for the management; it is undertaken at the instance of the management for providing it with information and appraisal of operations and activities. A parallel development in auditing is getting shaped as a management audit. Management audit is an "audit of the management" also.

The scope and content of management audit should cover everything that we know as operational audit and, in addition, it should also include a review of the adequacy and competence of the objectives, plans, policies and decisions of the top management.

IIA publication defines operational auditing as – "A systematic process of evaluating an organisation's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement."

Operational Audits involve undertaking a deep analysis of operations to bring out the improvement plan with respect to its overall standard of operation including improvement in effectiveness, efficiency, benefits vis-à-vis cost of operation, and its impact on meeting the objective of the operations and that of the organization.



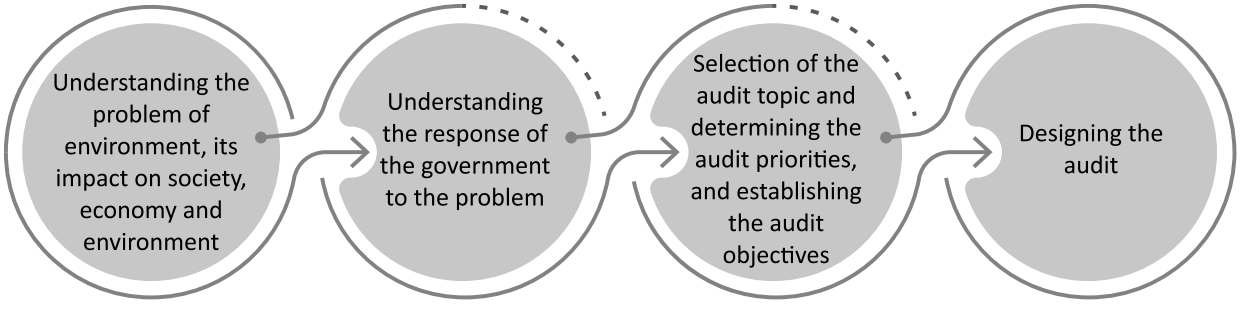
Compliance Audit: Compliance audit is an assessment as to whether the provisions of the applicable laws, rules and regulations made there under and various orders and instructions issued by the competent authority are being complied with. This audit by its very nature promotes accountability, good governance and transparency as it is concerned with reporting deviations, identifying weaknesses and assessing propriety.

ISSAI 4100 defines compliance audit as follows:

"Compliance audit deals with the degree to which the audited entity follows rules, laws and regulations, policies, established codes, or agreed upon terms and conditions, etc. Compliance auditing may cover a wide range of subject matters".

Environmental Audit: Defined as performance, compliance or financial audit addressing the approach taken by responsible bodies (e.g. government) to a specific environmental problem, or environmental policies, or programmes, as well as their performance in managing environmental issues.

Four Step Process



Performance Audit: Performance audit refers to an independent examination of a program, function, operation or the management systems and procedures of an entity to assess whether the entity is achieving economy, efficiency and effectiveness in the employment of available resources. The examination is objective and systematic, generally using structured and professionally adopted methodologies. The scope of performance audits may include the detection of fraud, waste and abuse.

Performance auditing in the public sector: a case study of Sri Lanka

Purpose – This study aims to investigate as to why the Auditor General's Department of Sri Lanka (AGD) needs a performance auditing (PA) system to enhance the public sector accountability system of the country. Further it aims to explore the ways and means of implementing a formal PA system. In so doing this study reviews the existing role of the AGD and its contribution to the enhancement of public accountability system of the country and examines the audit management functions and process of the AGD in the social, economic and political context of Sri Lanka within which the AGD operates.

Design/methodology/approach – New institutional sociological (NIS) theory framework, more specifically the institutional rational dynamic model developed by Dillard *et al.* (2004), was adopted to explore the broader social level criteria and forces which influence the auditing practices of the AGD. The case study research approach has been adopted as the research strategy. The data were collected through a total of 30 in-depth interviews using open-ended questionnaires and archival documents. The interviewees were selected from different management levels in the AGD.

Findings – The findings indicate that the practices of the AGD had not changed substantially, along with the social, economic and public administrative changes and developments that took place in the public sector auditing profession around the world. The factors such as the foreign donor's support for institutional developments in the AGD, lack of political support, bureaucratic influences, insufficient operational independence and traditional organisational culture of the AGD significantly affect the development of PA

practices at the AGD. Also the findings reveal that the audit management failures and resource constraints affected the existing practices of the AGD. The main rationale for implementing a formal PA system in the AGD is to enhance the public accountability system of the country. The findings also suggest that to achieve PA implementation task, the AGD has to depend on international assistance and has to negotiate with the political and public administrative authorities.

https://www.emerald.com/insight/content/doi/10.1108/jaoc.2010.31506dad.001/full/html

Special Audit: Special assignment audits are aimed at specific areas and aspects of the company operations which do not require comprehensive inspection of the entire system of accounting. It's a type of internal audit and is conducted only at the initiative of the organizations management and shareholders. The main purpose of this type of audit is the timely detection of errors and irregularities in the accounting and reporting as well as identifying additional possibilities for improving the efficiency of the business process.

Information Systems Audit: Information Systems Auditing or systems audit is an ongoing process of evaluating controls, collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. Thus, information systems auditing supports traditional audit objectives; attest objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that encompass not only attest objectives but also effectiveness and efficiency objectives. An information systems audit performed in an organization is a comprehensive examination of a given targeted system. The audit consists of an evaluation of the components which comprise that system, with examination and testing in the following areas:

- High-level systems architecture review
- Business process mapping (e.g. determining information systems dependency with respect to user business processes)
- End user identity management (e.g. authentication mechanisms, password standards, roles limiting or granting systems functionality)
- Operating systems configurations (e.g. services hardening)
- Application security controls
- Database access controls (e.g. database configuration, account access to the database, roles defined in the database)
- Anti-virus/Anti-malware controls
- Network controls (e.g. running configurations on switches and routers, use of Access control lists, and firewall rules)
- Logging and auditing systems and processes
- IT privileged access control (e.g. System Administrator or root access)
- IT processes in support of the system (e.g. user account reviews, change management)
- Backup/Restore procedures

QUALIFICATION AND APPOINTMENT OF INTERNAL AUDITOR

Who can perform Internal Audit

As per the provisions of Section 138 of the Companies Act 2013, companies are required to appoint an internal auditor [which may be either an individual or a partnership firm or a body corporate] who needs to be a professional. The said person can be a chartered accountant or a cost accountant, or a Company Secretaries or such other professional as may be decided by the Board.

The term professionals is a wider term which facilitates other professionals such as Company Secretaries or Lawyers to be appointed as internal auditors and to ensure timely compliance checks on a company. *The Internal auditor may or may not be an employee of the company.*

The board may appoint any practicing Chartered Accountant or a Cost Accountant (whether engaged in practice or not) or any other person whom it deems fit to be appointed as its internal auditor. For this purpose, company board may consider the nature and volume of business of company; qualifications, experience and capabilities of such person being appointed as auditor and scope of internal audit.

Note:

(a) Internal Auditor cannot be appointed by the Board by passing a resolution by circulation.

(b) Statutory Auditor shall not be appointed as internal auditor of the Company.

(c) A Cost Auditor of a Company shall not be the internal auditor of a Company for the period for which he is conducting the Cost Audit.

Procedure to be followed by the Company in the appointment of an Internal Auditor:

1. Obtain a written consent of the auditor for being eligible for appointment as an Internal Auditor under Companies Act, 2013.
2. Issuing 7 days' notice for calling a board meeting for appointment of internal auditor.
3. Hold board meeting and appoint internal auditor.
4. Inform the auditor about his appointment as an internal auditor of the company.
5. Filing form MGT-14 for appointment of internal auditor within 30 days of passing board resolution.
6. Send intimation to appointed Internal Auditor

The Audit Committee of the company or the Board shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity and methodology for conducting the internal audit.

CASE STUDY

1. The Management of XYZ Pvt. Ltd appointed Luthra and Co. (Chartered Accounting Firm) as an internal auditor of the company who is also a statutory auditor of the XYZ Pvt. Ltd. Is the appointment of Luthra and Co. (Chartered Accounting Firm) as an Internal Auditor of XYZ Pvt. Ltd. is valid?

Solution:

- As per section 138, the internal auditor shall either be a chartered accountant or a cost accountant (whether engaged in the practice or not), or such other professional as may be decided by the Board to conduct an internal audit of the functions and activities of the company.
- The internal auditor may or may not be an employee of the company. However, Statutory Auditor shall not be appointed as internal auditor of the Company.

Therefore, the appointment of Luthra and Co. (Chartered Accounting Firm) as an internal auditor of XYZ Pvt. Ltd. is not valid as Luthra and Co. is also a statutory auditor of XYZ Pvt. Ltd.

2. Few members of the Board of Directors oppose the appointment of Mr. N, an employee of the company, as an Internal Auditor, stating that Mr. N is not a chartered accountant and further he is an employee of the company

Solution:

Incorrect: As per section 138, the internal auditor shall either be a chartered accountant or a cost accountant (whether engaged in practice or not), or such other professional as may be decided by the Board to conduct internal audit of the functions and activities of the companies. The internal auditor may or may not be an employee of the company.

Illustration:

Internal Auditor is appointed by the _____

(a) Shareholders of the Company

(b) Statutory Auditor

(c) Institute of Internal Auditors of India

(d) Board of Directors of the Company

Correct Option: d) Board of Directors of the Company

Skill required to perform Internal Audit

The scope of the Internal Audit is continuously changing, transforming and evolving from fulfilling a watchdog function, with a focus on compliance audits, to one that now assesses financial controls for management and is management's eyes and ears. Internal auditors should possess and demonstrate through their work, actions and communication a number of traits, including, but not limited to:

- A commitment to and demonstration of competence in the field of Internal Auditing
- Strong financial and operational background in accounting, IT, regulatory compliance or the industry in which a company operates
- Honesty and Integrity
- Strong work ethic and attention

In general, internal auditors should develop and maintain a healthy level of professional skepticism and objectivity to assist in evaluating information and making judgments. Internal audit professionals should possess exceptional verbal and written communication skills, and be proficient in negotiating and reasoning with a variety of departments and groups over which internal audit may have no formal authority. Further personal integrity, professional due diligence and curiosity are important traits for individuals tasked with conducting internal audit work.

General Skills	*Specific Skills*
Technical Standards: The internal auditor should have adequate knowledge of the applicable Indian Accounting Standards and also in-depth knowledge on how to apply them in practice.	**Planning Audit Engagements:** This involves the ability to plan audit engagements on the basis of a comprehensive risk assessment prior to commencement of audit. The individual has to be experienced in the conduct of a brainstorming discussion on risk assessment. He should also have the necessary experience and capability to be able to preempt significant issues that might come up during the audit, needing greater focus.
Positive Attitude and Interpersonal Skills: The internal auditor should possess positive and objective attitude, free of any prejudice. He should posses good interpersonal and communication skills.	**Team Building:** This involves collecting people and facilitating coordination among them to ensure that they work as a unified team. It involves identification of team leaders, delegation of authority, motivating the team and communicating to them the results expected.
IT Skills: With the rapid proliferation of information technology (IT) in the accounting and other operational aspects of an entity, it is essential for an internal auditor to be able to work in an IT driven environment. Thus, it is essential that the internal auditor should either have or acquire sufficient knowledge of how information technology has been integrated in the functioning of the organization and also skills that would enable him to effectively use IT tools in carrying out a purposeful internal audit.	**Managing Audit Engagements**: This involves administration of the audit assignment. It involves the task of meeting auditees, understanding their expectations, communicating the engagement plan to them, selecting the right team, etc.
Interviewing Skills: Interviewing is the process of ascertaining information through verbal interaction with clients. It involves detailed questioning on various processes and procedures to ascertain whether the client's organization complies with the established standard operating procedure and practices and whether there is favorable or adverse variance from the standards, and in case of adverse variance what measures have been initiated by the management to ensure prevention of such adverse variances in future. Further, it is extremely important that the internal auditor and its team must be conversant with interviewing techniques so that appropriate questions could be asked in order to derive conclusion.	**Knowledge Management Skills**: An internal auditor either has or obtains sufficiently detailed knowledge of the operations of the entity as well as the constituents of the external environment in which the entity operates. For example, the industry, the regulators, the customers, etc. Some of this knowledge might be confidential and critical to the working of the entity. The internal auditor needs to have skills to effectively manage the knowledge, for example, deciding on issues such as: • collating the knowledge. • how and where to apply the knowledge. • assessing which team member needs what type and quantum of knowledge. • assessing when the knowledge has become obsolete and needs updating.

General Skills	*Specific Skills*
	• establishing the relationships between various pieces of knowledge and assessing how the same affects the internal audit. • deciding on manner and channels of flow of information. • Benchmarking Skills.
Audit Documentation Skills: Audit documentation is the process of compiling and filing of the findings of audit. It involves collating requisite documents as evidences for supporting audit findings, filing the analysis and supporting papers in a logical manner and assimilating information for presentation in a structured manner.	**Making Professional Presentations:** An experienced internal auditor should be able to make effective presentations to the Audit Committee. This would involve selecting and presenting the major issues that warrant senior management attention in a clear and unambiguous manner.
Reporting Skills: Reporting is the result of any audit assignment. It is therefore necessary that the audit report is written in such a manner that all issues are reported objectively and process gaps are addressed properly. It is also necessary that each observation is constructed in a manner that it represents the facts about the issue, its monetary or other impact, the cause of the issue and the suggestions for remedial actions and improvements.	

Besides the above skills, an Internal Auditor should also possess:

1. Analytical/Critical thinking skills
2. Data mining and Analysis Skills
3. Good Business Acumen and the ability to understand different business needs
4. He should have the ability to trace out facts and figures
5. Should be methodical and tactful while dealing with people and processes
6. Should be a hard worker, always cautious, vigilant and inquisitive
7. Should be courageous, assertive and determined with the ability to take independent decisions
8. Should lead by being punctual, reliable and updated with the latest knowledge and skill set.

STRATEGIC AND OPERATIONAL ROLE OF INTERNAL AUDITOR

Role of Internal Audit in Internal Control

The Internal auditor should examine and contribute to the ongoing effectiveness of the internal control system through evaluation and recommendations. However, the internal auditor is not vested with management's primary responsibility for designing, implementing, maintaining and documenting internal control. Internal audit functions add value to an organization's internal control system by bringing a systematic, disciplined approach to the evaluation of risk and by making recommendations to strengthen the effectiveness of risk management

efforts. The internal auditor should focus towards improving the internal control structure and promoting better corporate governance.

The role of the internal auditor encompasses:

- Evaluation of the efficiency and effectiveness of controls
- Recommending new controls where needed or discontinuing unnecessary controls
- Using control frameworks
- Developing Control self-assessment.

Role of Internal Audit in Risk Management

Internal auditing professional standards require the function to monitor and evaluate the effectiveness of the organization's Risk management processes. Risk management relates to how an organization sets objectives, then identifies, analyzes, and responds to those risks that could potentially impact its ability to realize its objectives. Under the COSO Enterprise Risk Management (ERM) Framework, risks fall under strategic, operational, financial reporting, and legal/regulatory categories. Management performs risk assessment activities as part of the ordinary course of business in each of these categories. Examples include: strategic planning, marketing planning, capital planning, budgeting, hedging, incentive payout structure, and credit/lending practices. Sarbanes-Oxley regulations also require extensive risk assessment of financial reporting processes. Corporate legal counsel often prepares comprehensive assessments of the current and potential litigation a company faces. Internal auditors may evaluate each of these activities, or focus on the processes used by management to report and monitor the risks identified. For example, internal auditors can advise management regarding the reporting of forward-looking operating measures to the Board, to help identify emerging risks.

In larger organizations, major strategic initiatives are implemented to achieve objectives and drive changes. As a member of senior management, the Chief Audit Executive (CAE) may participate in status updates on these major initiatives. This places the CAE in the position to report on many of the major risks the organization faces to the Audit Committee, or ensure management's reporting is effective for that purpose.

CASE STUDY

1. XYZ, a manufacturing unit does not accept the recommendations for improvements made by the Internal Auditor. Suggest an alternative way to tackle hostile management.

Solution:

While conducting the internal audit of a manufacturing unit, the auditor has to come across many irregularities and areas where improvement can be made and therefore he gives his suggestions and recommendations. These suggestions and recommendations for improvements may not be accepted by the hostile managers and in effect there may be cold war between the operational auditor and the managers.

This would defeat the very purpose of the internal audit. The Participative Approach comes to the help of the auditor. In this approach the auditor discusses the ideas for improvements with those managers that have to implement them and make them feel that they have participated in the recommendations made for improvements. By soliciting the views of the operating personnel, the internal audit becomes a co-operative enterprise. This participative approach encourages the auditee to develop a friendly attitude towards the auditors and look forward to their guidance in a more receptive fashion. When the participative method is adopted then the resistance to change becomes minimal, feelings of hostility disappear and gives room for feelings of mutual trust. Team spirit is developed. The auditors and the auditee together try to achieve the common goal. The proposed recommendations are discussed with the auditee and modifications as may

be agreed upon are incorporated in the internal audit report. With this attitude of the auditor, it becomes absolutely easy to implement the proposed suggestions as the auditee themselves take initiative for implementing and the auditor does not have to force any change on the auditee. Hence, the internal Auditor of XYZ manufacturing unit should adopt the above mentioned participative approach to tackle the hostile management of XYZ.

2. XYZ advisors is a management consulting firm having 250 fortune company client base. The CEO of the company is concerned about high employee attrition rate in his company. He has given assignment to dig out the reason for such high attrition rate as well as way forward. What factors would an Internal Auditor consider in such analysis?

Solution:

The following are the major factors responsible for high employee attrition rate are as under:

i. Job Stress & work life imbalance;

ii. Wrong policies of the Management;

iii. Unbearable behaviour of Senior Staff;

iv. Safety factors;

v. Limited opportunities for promotion;

vi. Low monetary benefits;

vii. Lack of labour welfare schemes;

viii. Whether the organization has properly qualified and experienced personnel for the various levels of works?

ix. Is the number of people employed at various work centers excessive or inadequate?

x. Does the organization provide facilities for staff training so that employees and workers keep themselves abreast of current techniques and practices?

Practice Question

1. **Should the organisation perform an internal audit?**

   Emerging risk, new regulation and increasing corporate governance demands are continuously adding to the Board's accountability and therefore, Independent, internal auditing can provide the insight – and oversight – a board needs to meet their governance responsibilities.

2. **What is the Board's role and responsibility with regards to their Internal Audit?**

   The Board should approve the appointment of Internal Auditor. There must be open communication, sufficient resources and clarity of expectations for the newly-appointed Internal Auditor. A strategy must be agreed upon – and implemented – through that relationship built to ensure the Internal Audit's function charter.

3. **Who is the Internal Audit team reporting to?**

   An internal auditing team works, most optimally, when it functions independently and objectively of a board. However, reporting to the Board – or, a Board-appointed Internal Audit committee – is another important step for the approval of audit plans and budgets, CAE appointments and all other decisions, including the: people, processes, technology and structure of the function as well as interpreting the Audit findings.

LESSON ROUND-UP

- Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes – Institute of Internal Auditors
- **Applicability:** As per section 138 of the Companies Act, 2013, following class of companies (prescribed in rule 13 of Companies (Accounts) Rules,2014) shall be required to appoint an internal auditor which may be either an individual or a partnership firm or a body corporate, namely-
  - (a) every listed public company;
  - (b) every unlisted public company having
    - (i) paid up share capital of fifty crore rupees or more during the preceding financial year; or
    - (ii) turnover of two hundred crore rupees or more during the preceding financial year; or
    - (iii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year; or
    - (iv) outstanding deposits of twenty five crore rupees or more at any point of time during the preceding financial year; and
  - (c) every private company having-
    - (i) turnover of two hundred crore rupees or more during the preceding financial year; or
    - (ii) outstanding loans or borrowings from banks or public financial institutions exceeding one hundred crore rupees or more at any point of time during the preceding financial year.
- Purpose of Internal Audit, Authority and Responsibilities of Internal Audit.
- The difference between Internal and External Audit.
- Types of Internal Audit
  - (i) Operational Audit
  - (ii) Compliance Audit
  - (iii) Environmental Audit
  - (iv) Performance Audit
  - (v) Special Audit
  - (vi) Information System Audit
- **Who could be an Internal Auditor** - As per the provisions of Section 138 of the Companies Act 2013, companies are required to appoint an internal auditor [which may be either an individual or a partnership firm or a body corporate] who needs to be a professional. The said person can be a chartered accountant or a cost accountant, or a Company Secretaries or such other professional as may be decided by the Board.
- Various Skill of Internal Auditor
- Strategic Role of Internal Auditor

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

1. Explain Internal Audit. How it is differ from Statutory Audit?
2. Who can be appointed as an Internal Auditor of a company?
3. Which types / categories of companies mandatorily required to appoint Internal Auditor?
4. Explain in brief the process to be followed with respect to the appointment of internal auditor?
5. Why Internal Audit is necessary? Does it give additional benefit to the organization already gets it financial audited from Statutory Auditor?
6. What are the basics or general skills required to be an internal auditor of a company?
7. What are the responsibilities of Internal Auditor?
8. Shree Pvt. Ltd. has outstanding loans or borrowings from banks Rs. 200 crores wants to appoint an internal auditor. Please guide him with respect to the applicability of the same.
9. What are the penalties for non-compliance with respect to appointment of internal auditor?
10. Briefly elaborate the role of Internal Auditor in Internal Control.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Practices related to Internal Auditing

Lesson 2

KEY CONCEPTS

■ Standards on Internal Audit 'SIA' ■ Corporate Social Responsibility 'CSR'

Learning Objectives

To understand:

- The Evolution of Internal Audit in India
- Several laws and regulations such as Companies Act, 2013, SEBI, RBI, IRDAI govern internal audit in India
- The laws of foreign government or regulators governing internal audit
- Section 138 of Companies Act, 2013 read along with Rule, 2014 impacting internal audit
- Who can be considered as 'Professional'
- Standards on Internal Audit 'SIA' in India
- The principles and governing framework of SIA
- International Standard issued by Institute of Internal Auditor 'IIA'
- Checklist for Corporate Social Responsibility 'CSR'

Lesson Outline

- Introduction
- Laws by Indian Government or Regulators Govern Internal Audit
- Laws by Foreign Governments or Regulators
- Specific Provisions under Companies Act, 2013 impacting Internal Audit
- Standards on Internal Auditing in India
- International Standards by Institute of Internal Auditors (IIA)
- Internal Audit Practices
- Corporate Social Responsibility
- Code of Ethics
- Environmental and Societal Safeguards
- Change Management
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION

In the previous lesson we have discussed about the key concepts and an overview about internal audit. In this chapter we will strive to understand the relevant regulations, applicable standards and generally accepted practices in the internal audit activity of an organisation.

Evolution of Internal Audit

Historically, wherever there has been a need for one person's property or assets being entrusted to another person, there has also been a need to keep some checks and balances upon the fidelity of the person so entrusted, to ensure that interests of the actual owner are protected. Even during the era of Maurya dynasty, Kautilya, a 4th century B.C.E. economist, is believed to have recognized the importance of accounting methods in economic enterprises and emphasised the role and importance of periodic audits.

Audit systems have always been in place in business organisations having a separation between people responsible for management of the day-to-day affairs and people having actual ownership of the organisation. Due to this principle, legal systems in most countries, including India, prescribe specific and detailed provisions in relation to auditing systems to be implemented to review a company's affairs. Thus, various regulations prescribe different audits for a company's affairs with specific scope and objectives from time to time.

With the increase in size and complexity of business activities within corporate organisations, annual statutory audit or tax audits were not perceived as enough to keep the right level of checks and balances. Thus, the Internal Audit systems were introduced in India by some progressive companies.

Recognizing its worth in achieving an independent view on financial information and supporting the assessment of a statutory auditor during financial statement audits, the internal audit in India was first made mandatory for a specific set of companies vide the Manufacturing and Other Companies (Auditor Report) Order, (MAOCARO, 1975). MAOCARO, 1975 required the statutory auditor to report whether the company has an internal audit system commensurate with its size and nature of its business and, whether there is an adequate internal control procedure commensurate with the size of the company and the nature of its business, for the purchase of stores, raw materials including components, plant and machinery, equipment and other assets, and for the sale of goods.

At that time, internal audit was thought to be subservient to statutory auditors having prime focus on the finance function and internal controls related to financial reporting and some legal compliances. The focus of internal audit at that time was to continuously audit financial records and related controls to provide an assurance that the financial controls are adequate and operating effectively. The statutory auditors used to rely on the assertions of the internal auditor.

With subsequent amendments in the law in MAOCARO, 1988 and later in CARO 2003, the mandatory requirement to have an internal audit system were further enhanced to apply to the producer companies in MAOCARO 1988, and later to all listed companies and other specified companies in CARO 2003.

The internal audit got further importance through clause 49 of listing agreement in the year 2005 wherein the audit committee of company was mandated to review the appointment of Chief Internal Auditor and to review internal audit reports related to internal control weaknesses. Further, with the latest requirements of Companies Act 2013, CARO 2020 and other relevant regulations, the importance of Internal Audit activity is increasing day by day. We shall discuss about the latest regulations later in this chapter.

Globally, Mr. Lawrence Sawyer (1911-2002) is often referred to as "the father of modern internal auditing" since he advocated the contemporary theory of Internal Auditing which is reflected in the current philosophy, theory and practice of internal auditing as defined by the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors. He had recommended the internal auditors to differ from classical compliance

auditing and take a different stance and a different state of mind, which is constructed on a foundation of technical excellence, and with the support from the highest levels of management in the organisation. The contemporary idea of internal auditing is thus to help an organisation accomplish its objectives.

LAWS BY INDIAN GOVERNMENT OR REGULATORS GOVERN INTERNAL AUDIT

There are several laws and regulations that govern internal audit related activities in India. Some of the key laws applicable to internal audit in India are:

- **Companies Act, 2013**: Section 138 of the Companies Act, 2013 mandates that certain classes of companies shall appoint an internal auditor who shall conduct an internal audit of the functions and activities of the company. These requirements are defined in Rule 13 of the Companies (Accounts) Rules, 2014.
- **Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements), Regulations 2015**: These regulations define requirements for listed companies' audit committee and their interaction with internal audit activity. They cover amongst others, reporting of internal audit, specific items to be reviewed in relation to internal audit, and audit committee interactions with internal auditors.
- **Reserve Bank of India (RBI) Guidelines**: The RBI has issued guidance note on Risk Based Internal Audit for various entities such as banks, non-banking financial companies (NBFCs), and payment system providers. These guidelines were amended in January 2021 and their applicability was extended to NBFCs, and UCBs also in February 2021.
- **Insurance Regulatory and Development Authority of India (IRDAI)** regulations has issued Guidelines for Corporate Governance for Insurers in India in 2009, which have been updated in 2016. These guidelines define the requirements for Board to lay down policy framework for control functions such as internal audit department, audit committee oversight on internal audit activity, and responsibilities of internal auditors.

While above are some of the key laws and regulations applicable to internal audit in India, there may be other laws and regulations specific to certain industries or sectors that may require internal audit.

Further, specific provisions in Companies Act 2013 and underlying Rules specify the requirements about stating whether the internal controls were adequate and effective during a financial reporting period by various corporate governance stakeholders such as Board, Audit Committee, Statutory Auditors etc., thus indirectly requiring an internal audit of internal controls on regular basis. We will discuss about these provisions in later sections of this chapter.

LAWS BY FOREIGN GOVERNMENTS OR REGULATORS

United States

In the United States, there is no specific law that mandates companies to conduct internal audits. However, there are various regulations and guidelines that require companies to have effective internal control systems in place. The Sarbanes-Oxley Act of 2002 (SOX) is one such regulation that mandates publicly traded companies to have a system of internal controls over financial reporting, and to evaluate and report the effectiveness of those controls.

The Public Company Accounting Oversight Board (PCAOB) is a regulatory body set up by the Sarbanes-Oxley Act 2002, that oversees the auditing profession and establishes auditing standards for public companies. The PCAOB requires statutory auditors to evaluate the effectiveness of a company's internal controls over financial

reporting during an audit and has defined a specific standard AS 2605 (Consideration of Internal Audit Function) to be adhered to by the statutory auditors. This standard lays down specific clauses defining the role of the auditor and the internal auditors, competence and objectivity of internal auditors, and effect of internal auditor's work on the statutory audit.

In addition to these regulations, many other regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Foreign Corrupt Practices Act (FCPA), Dodd-Frank Wall Street Reform & Consumer Protection Act, etc. mandate that companies have adequate internal controls, and they should be evaluated from time to time for effective implementation. Thus, indirectly internal audit's scope is drawn out by these regulations also.

Notably, the Securities and Exchange Commission (SEC) does not have any specific rules or regulations related to internal audit and it does not specifically regulate internal audit. The Institute of Internal Auditors has however given a framework of IPPF (International Professional Practices Framework) which is used by internal auditors to be able to demonstrate that their internal audit practices are in line with the global standards.

Japan

In Japan, the Companies Act does not specifically require companies to have an internal audit function, but it does require them to have an internal control system. Many companies in Japan choose to establish an internal audit function as part of their internal control system.

A KK (kabushiki kaisha) is the most common form of corporate entity in Japan. As of 31 July 2021, 92.1% of Japanese corporate entities were KKs. KKs are generally classified according to the transfer restrictions imposed on their shares: Close KKs (private companies) and Open KKs (public companies). In Japan, corporate governance and directors' duties are regulated by the Companies Act and a Company's articles. Further, in case of listed KKs, The Financial Instruments and Exchange Law and Securities Listing Regulations published by the securities exchanges (including the Corporate Governance Code) are also applicable.

The Financial Instruments and Exchange Act (popularly known as J-SOX) is the set of Japanese standards for evaluation and auditing of internal controls over financial reporting also referred to as "the Standards", were finalized on February 15, 2007. Based on the Standards' requirements, all listed companies in Japan are to perform risk assessments and prepare and submit internal control reports on a consolidated basis. J-SOX requirements are the Japanese equivalent to U.S. SOX. This entails that controls need to be tested thoroughly, and internal audit departments are usually helping the management in doing so.

Generally, in Japan the Corporate governance and directors' duties are regulated by:

- The Companies Act
- A company's articles.

In addition, for listed KKs below regulations are also applicable:

- The Financial Instruments and Exchange Law.
- Securities Listing Regulations published by the securities exchanges (including the CG Code).

The Ministry of Justice is the administrative authority in charge of the Companies Act and The Financial Services Agency (FSA) is the authority in charge of the Financial Instruments and Exchange Law, and regulation of listed KKs.

France

In listed companies, the chairperson of the Board states about internal control and risk management procedures

put in place by the company in the annual report. Specific focus on the controls related to the preparation of accounting / financial information is required. The legal auditors (statutory auditors) must also provide their observations on the chairperson's report. Thus, internal audit functions are usually set up in all listed companies, although not required mandatorily.

The corporate governance legislation in France is the French Commercial Code (Commercial Code), which provides rules covering the composition, powers, remuneration, duties and liabilities of a company's governing bodies.

The main corporate governance code referred to by the listed companies in France is the Afep-Medef Code (A-M Code), published by the two main French business federations *(French Association of Private Enterprises and French Enterprise Movement)- (Association Française des Entreprises Privées and Mouvement des Entreprises de France) - (Afep and Medef).* Another corporate governance code, the Middlenext Code, is mainly used by small and medium-sized listed companies.

The body responsible for monitoring the implementation of the A-M Code is the High Committee for Corporate Governance *(Haut Comité de gouvernement d'entreprise)* (HCGE), which publishes a practice guide for the A-M Code and an annual report on compliance by French listed companies in the SBF 120 with the A-M Code.

The main representative body for shareholders in France that monitors corporate governance is the Association for the Defence of Minority Shareholders (Association de défense des actionnaires minoritaires) (ADAM).

China

Listed companies in the People's Republic of China (PRC) are required to establish internal control systems in accordance with the stock exchange rules and Basic Internal Control Norms for Enterprises (BICNE) within a fixed timetable. The directors of listed companies are responsible and liable for information disclosed in the various reports, including fiscal reports. Thus, although there are no specific requirements for internal audit, the role of internal audit is derived by the assurance needed by the directors. Internal audits are thus applicable for listed companies, state-owned enterprises (SOEs), and governmental agencies.

While relatively new in comparison to guidelines recognized globally, China has an evolving regulatory framework for internal controls and audit. China-SOX (Basic Standard) which is China's version of the US Sarbanes-Oxley Act of 2002 was issued in 2008, with supporting guidelines issued in 2010. The Basic Standard for Enterprise Internal Control (*caikuai* [2008] No. 7, "Basic Standard") mirrors its US counterpart mostly. Further, to implement the Basic Standard, in April 2010, the five Chinese governmental departments issued the Supporting Guidelines for Internal Control of Enterprises (*caikuai* [2010] No.11, "Supplementing Guidelines").

The Supplementing Guidelines consist of three guidelines:

- Application Guidelines
- Evaluation Guidelines
- Audit Guidelines

The Supplementing Guidelines require listed companies and non-listed large and medium-sized enterprises governed by the Basic Standards and the Supplementing Guidelines to disclose an annual self-evaluation report on the effectiveness of their internal control as well as engage an accounting firm to issue an auditor's reports on the effectiveness of their internal control in financial reporting.

Currently the main legislations in China with respect to overall Corporate Governance are as follows:

- The Foreign Investment Law of the PRC, which applies to all foreign-funded enterprises.
- The Company Law, which applies to all corporate entities.

- The Securities Law of the PRC, which mainly applies to public companies, whether listed or not.
- Measures for the Supervision and Administration of State-owned Equities of Listed Companies, to regulate changes in state-owned shares of listed companies.
- Various regulations, measures and guiding opinions, including but not limited to the CG Code, issued by the CSRC and other authorities, which apply to listed companies.
- Various laws and regulations governing corporate governance of state-owned enterprises (SOEs).
- Various Stock Listing Rules issued by Shenzhen/Shanghai Stock Exchange to regulate the listing and information disclosure etc. of CLSs.

SPECIFIC PROVISIONS UNDER COMPANIES ACT, 2013 IMPACTING INTERNAL AUDIT

This section discusses the provisions of Companies Act, 2013 with respect to Internal Auditing in detail.

To start with, Section 138 of the Companies Act read along with Rule 13 of The Companies (Accounts) Rules, 2014 lays down that:

(1) Prescribed class or classes of companies shall be required to appoint an internal auditor, who shall either be a chartered accountant (whether in practice or not) or a cost accountant (whether in practice or not), or such other professional as may be *decided by the Board* to conduct internal audit of the functions and activities of the company. These companies are:

- every listed company.
- every unlisted public company having-
  - paid up share capital of 50 crore rupees or more during the preceding financial year, or
  - turnover of 200 crore rupees or more during the preceding financial year; or
  - outstanding loans or borrowings from banks or public financial institutions (PFIs) exceeding 100 crore rupees or more at any point of time during the preceding financial year; or
  - outstanding deposits of 25 crore rupees or more at any point of time during the preceding financial year; and
- every private company having-
  - turnover of 200 crore rupees or more during the preceding financial year; or
  - outstanding loans or borrowings from banks or PFIs exceeding 100 crore rupees or more at any point of time during the preceding financial year.

(2) The internal auditor so appointed may be either an individual or a partnership firm or a body corporate. Further, internal auditor may or may not be an employee of the company.

(3) The Audit Committee of the company (where it exists) or the Board shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity and methodology for conducting the internal audit.

The word **'professional'** is defined in Black's Law Dictionary [9th Edition, Page 1329] as "A person who belongs to a learned profession or whose occupation requires a high level of training and proficiency". Further, 'profession' is defined [9th Edition, Page 1329] as "A vocation requiring advanced education and training". A reading of this definition along with the above given legal provisions indicate that professionals such as qualified company secretaries, postgraduates in finance, etc. can be appointed as the internal auditors by the Board. However, it has to kept in view that the necessary skills and knowledge needs to be evaluated by the Board before such appointment.

Given the fact that Section 138 is placed within Chapter IX (Accounts of Companies) and the Rule 13 is placed under The Companies (Accounts) Rules, 2014, through harmonious reading of provisions it appears that a good level of knowledge about finance and accounting is a reasonable expectation for the appointment of an internal auditor. This, however does not mean that internal audit is required to focus on financial aspects only. Especially with advancement in the newer technologies such as AI/ML, the expectations of the regulators may change in recent future.

As mentioned above, the scope, functioning, periodicity and methodology of the internal audit needs to be formulated by Audit Committee or by the Board, in consultation of the Internal Auditor, a reference is required to be made to the good practices / standards of the internal audit profession, so that the Audit Committee or Board can rely upon such good practices / standards to deliver their responsibility in an effective manner. We will discuss about such good practices and standards in later sections of this chapter.

Further to above, the Companies Act also defines specific requirements with respect to Internal Financial Controls in various sections which have a bearing on the internal audit activity indirectly, some of them are discussed below:

1. **Section 134(3)(q) read with Rule 8(5) (IFCoFR) - Chapter IX-The Companies (Accounts) Rules, 2014**

   These rules require the details in respect of adequacy of internal financial controls with reference to the Financial Statements to be included in the Board's Report of all companies. These controls are usually known as Internal Controls on Financial Reporting - IFCoFR and form a subset of overall Internal Financial Controls of a company.

2. **Section 134(5) (Director's Responsibility Statement)**

   As per Explanation to Section 134(5)(e), for the purposes of this clause, the term internal financial controls (IFC) means the policies and procedures adopted by the company for ensuring the *orderly and efficient* conduct of its business, including adherence to company's policies, the safeguarding of its *assets*, the prevention and detection of *frauds and errors*, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information. This means that IFC covers not just the financial reporting aspects, but also the strategic and operational aspects of business and the efficiency with which those operations are carried out.

   Section 134(5)(e) requires the directors of a *listed* company to state whether they had laid down the internal financial controls, and whether these controls were adequate and working effectively during the financial year.

   Further, Section 134(5)(f) requires the directors to state if they had devised proper systems to ensure compliance with the provisions of all applicable laws and that such systems were adequate and operating effectively during the financial year. Note that this requirement is for *all companies*, and not only listed companies.

   Board of directors certainly need to review the design and operating effectiveness of internal controls before they can make a statement on their status as required by above given provisions, meaning thereby that testing of internal controls is needed, which is carried out by the internal auditors. Note that internal audit is responsible only for the testing the controls, and the formulation or revision of internal controls is the responsibility of the relevant function heads, and the executive management.

3. **Section 177, Subsection (4), (5) - Audit Committee**

   Section 177(4) requires that every Audit Committee, shall act in accordance with the terms of reference specified in writing by the Board which shall include evaluation of internal financial controls (IFC) and risk management systems.

Thus, in case of companies which are required to have an Audit Committee, the audit committee is required to evaluate the IFC and risk management systems. Notably, every listed public company and every other company covered under rule 4 of the Companies (Appointment and Qualification of Directors) Rules, 2014 is required to constitute an Audit Committee. Further, Section 177(5) requires that the Audit Committee may call for the comments of the statutory auditors about internal control systems, the scope of audit, including the observations of the auditors and review of financial statement before their submission to the Board and may also discuss any related issues with the internal auditors and statutory auditors and the management of the company.

Thus, internal auditors as well as statutory auditors are invariably asked to give comments by the audit committee on the IFC and risk management systems of the company. Considering this, evaluation of internal financial controls and risk management systems is assigned to internal auditors in most of the companies.

4. Section 143(3) – Powers and duties of auditors

Section 143(3)(i) of the Companies Act requires that the auditor's report shall also state whether the company has adequate internal financial controls system in place and comment on the operating effectiveness of such controls.

It is worth noting that as per Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Institute of Chartered Accountants of India (ICAI), consistent with the practice prevailing internationally, the term 'internal financial controls' stated in Section 143(3)(i) would relate to 'internal financial controls over financial reporting' in accordance with the objectives of an audit stated in SA 200 "Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with Standards on Auditing".

Further, as per the ICAI Guidance note on Audit of Internal Financial Controls Over Financial Reporting, the statutory auditor should evaluate the extent to which he or she will use the work of others to reduce the work the auditor might otherwise perform himself or herself. SA 610 "Using the Work of Internal Auditors" and SA 620 "Using the Work of an Auditor's Expert" apply in a combined audit of internal financial controls over financial reporting and financial statements. Further, irrespective of the degree of autonomy and objectivity of the internal audit function, such function is not independent of the entity as is required of the auditor when expressing an opinion on financial statements and internal financial controls over financial reporting. The auditor has sole responsibility for the audit opinion expressed, and that responsibility is not reduced by the auditor's use of the work of the internal auditors.

5. Section 143(11) – Companies (Auditor's Report) Order, 2020

Companies (Auditor's Report) Order, 2020 is issued under Section 143(11) and is also popularly known as CARO 2020. It applies to all companies including foreign companies except:

- a banking company as defined in section 5(c) of Banking Regulation Act, 1949
- an insurance company as defined under the Insurance Act, 1938
- a company licensed to operate under section 8 of the Companies Act
- a One Person Company as defined in section 2(62) of the Companies Act
- a small company as defined in section 2(85) of the Companies Act; and
- a private limited company,
    - ➢ not being a subsidiary or holding company of a public company, having a paid-up capital *and*

- reserves and surplus not more than 1 crore rupees as on the balance sheet date *and*
- which does not have total borrowings exceeding 1 crore rupees from any bank or financial institution at any point of time during the financial year *and*
- which does not have a total revenue as disclosed in Scheduled III to the Companies Act (including revenue from discontinuing operations) exceeding 10 crore rupees during the financial year as per the financial statements.

As per CARO 2020 Rule 3(xiv), the statutory auditor's report on the accounts of a company to which this Order applies shall include a statement on the following matters, namely:

- whether the company has an internal audit system commensurate with the size and nature of its business.
- whether the reports of the Internal Auditors for the period under audit were considered by the statutory auditor.

ICAI has issued a Guidance Note on The Companies (Auditor's Report) Order, 2020. As per this Guidance Note, the auditor needs to examine the following aspects to evaluate whether the internal audit system is commensurate with the size of the company and the nature of its business :

(i) ***The size of the internal audit department*** considering the nature of the business of the company, the number of operating locations, the extent to which internal controls are decentralised, the effectiveness of other forms of internal control, etc.

(ii) ***Qualifications of the persons who undertake the internal audit work*** is a necessary aspect to be reviewed to ensure that there are adequate number of qualified personnel. In cases where external agencies are appointed, the auditor would need to evaluate their competency, objectivity and the independence. The auditor may do this by assessing the qualifications, experience and the professional standing.

(iii) ***Reporting responsibility of the internal auditor****:* It is expected that the internal auditor would report to those charged with governance. Under Companies Act, 2013, the internal auditor reports to the Board/ Audit Committee as per section 138. In case of listed companies, compliance of provisions of SEBI LODR Regulations with regards to review of internal audit function by audit committee, presence of head of internal audit in the audit committee meetings, audit committee involvement in appointment, removal and terms of remuneration of the chief internal auditor, a direct communication link between the internal auditor and audit committee, etc. shall be verified by the auditor.

(iv) ***Involvement of Board or Audit Committee in formulation of scope, functioning, periodicity and methodology of Internal Audit*** shall be examined by the auditor. As per guidance note, it is a good practice that statutory auditors are also involved by the internal auditor/ those charged with governance in determining the scope of work and periodicity of reporting.

(v) ***Technical assistance to the internal auditor****:* In companies where the operations are highly technical or automated in nature, an internal auditor cannot function effectively unless he has adequate technical assistance. Statutory auditor shall review the availability of technically qualified persons (either full time or assignment based).

(vi) ***Reports submitted by the internal auditor****.*

(vii) ***Existence of adequate follow-up system*** to ensure that the deficiencies pointed out are corrected and remedial action taken on the deficiencies are reported upon.

(viii) ***Minutes of the meetings of the Board of Directors and audit committee*** to get useful evidence regarding the efficiency and efficacy of the internal audit system.

(ix) Existence or otherwise of other forms of internal control*:* Internal audit system is a part of the overall internal control system. Therefore, the scope of the internal audit and the extent of its coverage will, to some extent, depend upon the existence or otherwise of other forms of internal control. This is also a factor to be considered when evaluating the adequacy of the internal audit system.

(x) If the statutory auditor determines that the internal audit system is not commensurate with the size and nature of business of a company, then the auditor should communicate with the Audit Committee or Board and seek their inputs as part of "Communication to Those Charged with Governance" and accordingly report the fact under this report.

Similarly, some of the other aspects that a statutory auditor needs to consider while reporting whether the reports of the Internal Auditors for the period under audit were duly considered by him / her are given below:

(i) Internal audit is completed as per the plan and the reports are made available sufficiently in time. In case required, a meeting with internal auditor to discuss the observations to independently evaluate the impact of the observations on the financial statements has been done.

(ii) All internal audit observations having a financial impact are considered by the management and control deficiencies pointed out by the internal auditors are rectified.

(iii) Impact of the control deficiencies, if any, pointed by the internal auditors on internal financial controls over financial reporting (IFCoFR) have been assessed by auditor.

(iv) Since auditor is vested with the right to receive the full-fledged internal audit reports (including draft audit reports) together with annexures and not merely the executive summary / power point presentations, whether the same were made available when requested.

Considering the above requirements, *it becomes obligatory for a company to implement robust internal audit system, and demonstrate the same to statutory auditors,* failing which an adverse communication can be reported in the auditor's report. Thus, these requirements need to be kept in mind by the company when devising the policies and procedures in relation to internal audit system.

STANDARDS ON INTERNAL AUDITING IN INDIA

Since the law has left the task of formulation of scope, functioning, periodicity, and methodology for conducting an internal audit to audit committees or the board of directors in consultation with internal auditor, there is a clear need for adoption of uniformly acceptable practices in this regard.

This is required to ensure that internal auditor as well as the board or audit committee can demonstrate the effectiveness of internal audit activity to various stakeholders such as regulators, statutory auditors etc. in a confident and objective manner, by following a set of minimum requirements that are followed widely by the industry within internal audit fraternity.

Considering that none of the internal audit related standards are mandated by law in India, the audit committee or the board needs to decide on which standards they plan to use. There are two standards that are widely used by companies in India:

- Standards on Internal Audit (SIAs), issued by Institute of Chartered Accountants of India.
- International Standards for the professional practice of Internal Auditing, issued by the Institute of Internal Auditors, USA.

Both these standards are based on similar principles about the concept of internal auditing. However, there are aspects which can be different from each other. Thus, an internal auditor needs to understand these standards well before making a proposal to adopt any of them by the audit committee or board.

Below is an overview of the national standards as formulated by ICAI. These standards are recommendatory for all the members of the Institute of Chartered Accountants of India. However, once a standard is adopted by a company's board or audit committee, then it becomes mandatory for that specific company.

National Standards: SIAs by ICAI

- **Preface** to the Framework and Standards on Internal Audit
- **Framework** Governing Internal Audits
- **Basic Principles** of Internal Audit
- **100 Series – Standards on Key Concepts**
  - SIA 110 – Nature of Assurance
  - SIA 120 – Internal Controls
  - SIA 130 – Risk Management
  - SIA 140 – Governance
  - SIA 150 – Compliance with Laws and Regulations
- **200 Series – Standards on Internal Audit Management**
  - SIA 210 – Managing the Internal Audit Function
  - SIA 220 – Conducting overall Internal Audit Planning
  - SIA 230 – Objectives of Internal Audit
  - SIA 240 – Using the Work of an Expert
  - SIA 250 – Communication with those charged with Governance
- **300 – 400 Series – Standards on Conduct of Audit Assignments**
  - SIA 310 – Planning the Internal Audit Assignment
  - SIA 320 – Internal Audit Evidence
  - SIA 330 – Internal Audit Documentation
  - SIA 350 – Review and Supervision of Audit Assignments
  - SIA 360 – Communication with Management
  - SIA 370 – Reporting Results
  - SIA 390 – Monitoring and Reporting of Prior Audit Issues
- **500 Series – Standards on Specialised Areas**
  - SIA 520 – Internal Auditing in an Information Technology Environment
  - SIA 530 – Third Party Service Provider

The SIA standards are similar in nature to the International Standards for the Professional Practice of Internal Auditing (IIA standards). However, the SIA standards have been tailored to the specific needs of the Indian environment and take into account the legal and regulatory requirements in India.

As per the Preface of SIAs, the Council of ICAI has decided that the Standards will be made mandatory in a

phased manner. The mandatory status of a SIA implies that while carrying out an internal audit, it shall be the duty of the members of the Institute to ensure that they comply with the SIAs read with the Preface, Framework Governing Internal Audits and Basic Principles of Internal Audit.

If, for any reason, a member is unable to comply with any of the SIAs requirements, or if there is a conflict between the SIA and other mandates, such as a regulatory requirement, the internal audit report (or such similar communication) should draw attention to the material departures therefrom along with appropriate explanation.

SIAs are principle based and clearly outline the objective of issuing the Standard along with the essential requirements for its compliance. Internal Auditors shall apply their best professional judgement in the implementation of SIAs on a "substance over form" basis. Implementation and Technical guides issued by the Board would help to provide the necessary guidance and clarification in this regard.

Every SIA is divided into following 5 sections:

(1) Introduction: brief background, scope, applicability.

(2) Objective: Reasons for issuing the Standard

(3) Requirements: The desired outcome and what is essential to ensure compliance with the Standard.

(4) Explanatory Comments on Implementation and Application: Certain parts of the Standard which needs to be elaborated, including defining key words and terms.

(5) Effective Date: Date from which the Standard is to be applied and made mandatory.

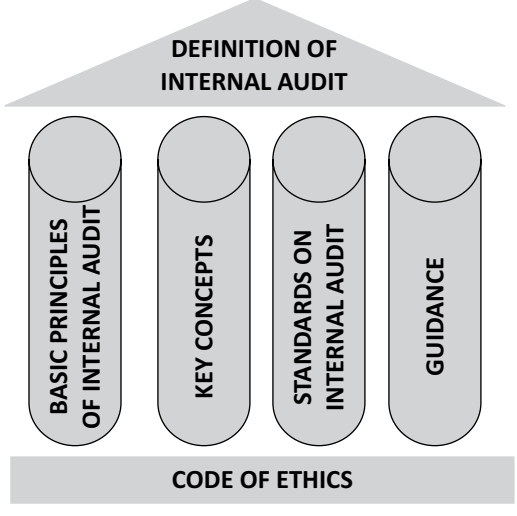
The **Governing Framework of SIAs** defines four components / pillars:

(i) Basic Principles of Internal Audit

(ii) Key Concepts

(iii) Standards on Internal Audit (SIAs)

(iv) Guidance.



Source: Governing Framework on SIAs by ICAI

As per the Governing Framework of SIAs, every Internal Auditor is bound by a written Code of Ethics, issued by an organisation and/or the professional institution of which he is a member. This commits the Internal Auditor to ethical Standards applied with utmost integrity and sincerity.

Thus, in case a company's board or audit committee decides to adopt SIAs as the standards for their organisation, the Internal Audit Manuals should reflect the requirements of not only the organisation, but also the above requirements as part of code of ethics of the Internal Audit department.

The Governing Framework of SIAs further defines the basic principles of Internal Audit, which is a set of core principles fundamental to the function and activity of internal audit. The Basic Principles are critical to achieve the desired objectives as set out in the Definition of the Internal Audit, and therefore, apply to all internal audits.

The principles can be summarised as follows:

Principles establishing the credibility of the internal auditor:

1. Independence
2. Integrity and Objectivity
3. Due Professional Care
4. Confidentiality
5. Skills and Competence

Principles outlining the elements which are essential for performance of internal audit activities:

6. Risk Based Audit
7. Systems and Process Focus
8. Participation in Decision Making
9. Sensitive to Multiple Stakeholder Interests
10. Quality and Continuous Improvement.

Let us understand these principles in brief now:

1. **Independence:**
    - The Internal Auditor shall be free from any undue influences which force him to deviate from the truth. This independence shall be not only in mind, but also in appearance.
    - Internal auditor shall resist any undue pressure or interference in establishing the scope of the assignments or the manner in which these are conducted and reported, in case these deviate from set objectives.
    - The independence of the internal audit function as a whole, and the Internal Auditor within the organisation, plays a large part in establishing the independence of the Internal Auditor. The overall organisation structure of key personnel, the position and reporting of the Chief Internal Auditor within this structure, along with the powers and authority which is derived from superiors further establishes the independence of the Internal Auditor.
    - The reporting of the Internal Auditor shall be to the Board of Directors, or the Audit Committee, who are responsible to appoint the Internal Auditors as per Rule 8 of "The Companies (Meetings of Board and its Powers) Rules, 2014". Many times, the Internal Auditor has a dual reporting responsibility, wherein the administrative reporting is to an executive officer (e.g., MD or CEO), but functional reporting to the Chairman of the Audit Committee, which is the acceptable norm. Therefore, the internal audit function shall be positioned outside the functions which are subject to internal audit (e.g., Finance and Accounts) and the Internal Auditor shall report directly to the highest governing body of the Company as stated above.

- At times, the Internal Auditor is exposed to a different type of risk to independence, whereby management seeks active business support from the Internal Auditor. Apart from providing basic assurance and advisory inputs, the Internal Auditor is assigned certain operational responsibilities (such as risk management, compliance, system automation, process re-engineering, etc.). Although some limited operational role may be acceptable with due approvals, and for a short duration, the Internal Auditor shall do so only after communicating his limitations along the following lines:

  (a) Unable to assume ownership or accountability of the process; and

  (b) Inability to take operational decisions which may be subject to an internal audit later on.

An argument may be made that an internal auditor, being an employee of the company cannot be independent since there may be occasions where pressures from management or conflicts of interest could arise, impacting the independence. Essentially, the concept of independence in a statutory audit and internal audit is different. While a statutory auditor needs to be completely independent of the company he is auditing, an internal auditor needs to be independent of the activities or departments that he is auditing. To ensure this independence the SIAs have recommended the position and reporting structure which makes internal audit reporting to the highest levels of governance in a company. Further, where the management asks internal auditor to assume additional roles and responsibilities that may impair, or appear to impair, the organizational independence of the internal audit activity, the same should be reported to the audit committee and board as well.

2. Integrity and Objectivity

- The Internal Auditor shall be honest, truthful and be a person of high integrity. He shall operate in a highly professional manner and seen to be fair in all his dealings. He shall avoid all conflicts of interest and not seek to derive any undue personal benefit or advantage from his position.
- The Internal Auditor shall conduct his work in a highly objective manner, especially in gathering and evaluation of facts and evidence.
- He shall not allow prejudice or bias to override his objectivity, especially in arriving at conclusions or reporting his opinion.

3. Due Professional Care

- The Internal Auditor shall exercise due professional care and diligence while carrying out the internal audit. “Due professional care” signifies that the Internal Auditor exercises reasonable care in carrying out the work to ensure the achievement of planned objectives.
- The Internal Auditor shall pay particular attention to certain key audit activities, such as establishing the *scope* of the engagement to prevent the omission of important aspects, recognizing the *risks and materiality* of the areas, having required *skills* to review complex matters, establishing the extent of testing required to achieve the objectives within specified deadlines, etc.
- “Due Professional Care”, however, neither implies nor guarantees infallibility, nor does it require the Internal Auditor to go beyond the established scope of the engagement. Where an internal auditor can demonstrate that the SIAs were followed while conducting the internal audit activity, due professional care is taken care of.

4. Confidentiality

- The Internal Auditor shall at all times, maintain utmost confidentiality of all information acquired during the course of the audit work.

- He shall not disclose any such information to a party outside the internal audit function and any disclosure shall be on a "need to know basis".
- The Internal Auditor shall keep confidential information secure from others. Under no circumstance any confidential information shall be shared with third parties outside the company, without the specific approval of the Management or Client or unless there is a legal or a professional responsibility to do so (e.g., to share information with Statutory Auditors).
- Internal audit reports shall be addressed to specified internal auditees and distributed to only those who appointed or engaged the Internal Auditor and as per their directions.

Compliance to above requirements of SIAs is both behavioural and process driven. For instance, while it is up to individuals to ensure confidentiality of information acquired during internal audit, the internal audit manual should specify the procedures to identify the people to be included in the distribution list of an internal audit report.

5. Skills and Competence

- The Internal Auditor shall have sound *knowledge*, strong *interpersonal skills*, practical *experience* and professional *expertise* in certain areas and other competence required to conduct a quality audit. He shall undertake only those assignments for which he has the requisite competence.
- The Internal Auditor shall either have, or shall obtain, such skills and competencies, as necessary for the purpose of discharging his responsibilities. Continuing Professional Education is a key part of this exercise.
- In addition to the basic technical skills, the Internal Auditor shall have the softer skills (such as interpersonal and communication skills) required to engage with a multitude of stakeholders.
- Where the Internal Auditor lacks certain expertise, he shall procure the required skills either though in-house experts or through the services of an outside expert, provided independence is not compromised.
- The objective is to ensure that the audit team, as a whole, has all the expertise and knowledge required for the area under review.

Compliance to above Principles of SIAs can be ensured by continuous upgradation of knowledge about the relevant laws, auditing related tools or technologies, and also the knowledge about the changes in company organisation, processes, IT systems etc. As a good practice, internal auditors should have an allocated annual budget for their training and skills enhancement. Interpersonal skills play a very important role in the internal audit activity, and thus developing these skills is necessary for every internal auditor. This principle also lays down that internal auditor should take help from other experts where he lacks expertise. For instance, while doing an internal audit of a construction project, including a civil engineer as part of the internal audit team is very much in line with SIAs requirement.

6. Risk Based Audit

- The Internal Auditor shall identify the important audit areas through a risk assessment exercise and tailor the audit activities such that the detailed audit procedures are prioritised and conducted over high-risk areas and issues, while less time is devoted to low risk areas through curtailed audit procedures.
- Additionally, this approach shall ensure that risks under consideration are more aligned to the overall strategic and company objectives rather than narrowly focused on process objectives.

- A risk-based audit shall ensure the following three-fold objectives:
  a) Audit procedures need not cover the whole process and can be limited only to the important controls in the process;
  b) Establish linkage to the aspects relevant and connected with company and functional objectives; and
  c) Findings and issues highlighted are significant and important and time is not devoted to areas with low probability of significant observations.

7. System and Process Focus

- An Internal Auditor shall adopt a system and process focused methodology in conducting audit procedures. This methodology is more sustainable than the one adopted to test transactions and balances as it goes beyond "error detection" to include "error prevention".
- It requires a root cause analysis to be conducted on deviations to identify opportunities for system improvement or automation, to strengthen the process and prevent a repetition of such errors.
- Deployment of Information Technology by companies is widely prevalent and should be understood for effective internal audits. This is a more sustainable approach as this helps the Internal Auditor to move away from "people to process" and from "detection to prevention".

8. Participation in Decision Making

- In conducting internal audit assignments, the Internal Auditor shall avoid passing any judgement or render an opinion on past management decisions.
- As part of his advisory role, the Internal Auditor shall avoid participation in operational decision making which may be subject of a subsequent audit.
- The focus of the Internal Auditor shall remain with the quality and operating effectiveness of the decision-making process and how best to strengthen it, such that the chance of flawed or erroneous decisions is minimised.
- However, the Internal Auditor is at full liberty to present the lessons which can be learnt from such past decisions.

This Principle lays down the boundaries or safeguards for internal auditors so that they are not perceived to have participated in the management decision making.

9. Sensitive to Multiple Stakeholder Interests

- The Internal Auditor shall evaluate the implications of his observations and recommendations on multiple stakeholders, especially where diverse interests may be conflicting in nature. In such situations, the Internal Auditor shall remain objective and present a balanced view.
- This would permit senior management to make a decision using all the information and balance the strategy and objectives of the company with the expectations and interests of its multiple stakeholders.

10. Quality and Continuous Improvement

- The quality of the internal audit work shall be paramount for the Internal Auditor since the credibility of the audit reports depends on the reliability of reported findings.
- The Internal Auditor shall have in place a process of quality control to:
  a) ensure factual accuracy of the observations;

b) to validate the accuracy of all findings; and

c) continuously improve the quality of the internal audit process and the internal audit reports.

- The Internal Auditor shall ensure that a self-assessment mechanism is in place to monitor his own performance and also that of his subordinates and external experts on whom he is relying to complete some part of the audit work.
- A peer review mechanism for quality control shall be followed to adhere to all aspects of the pronouncements issued by the ICAI.

Above discussion on the Preface, Governing Framework and Basic Principles of Internal Audit gives the required conceptual clarity and foundation to an internal auditor while performing his tasks. The specific standards (100 ~ 500 series) further elaborate and bring clarity on how to deal with various real-life situations as an internal auditor.

STANDARDS ON INTERNAL AUDIT ISSUED BY ICAI

100 Series: Standards on Key Concepts

Standard on Internal Audit (SIA) 110- Nature of Assurance

Deals with those assignments performed by internal auditors where an opinion is required, and it clarifies the minimum requirements to be in place before an audit opinion report can be issued.

This Standard covers only those assignments where an opinion is expressed through an internal audit report. An audit rating of an individual audit observation (e.g. for severity of outcome) or a risk rating of the audit observation, is not considered an audit opinion for the purpose of this SIA. An assurance assignment may be part of another project, for example, a Certification on Internal Controls over Financial Reporting. In such circumstances, this Standard is relevant only to the assurance portion of the assignment.

Standard on Internal Audit (SIA) 120- Internal Controls

This Standard applies to all internal audits conducted where internal controls are subject of audit review, and are being assessed, evaluated and reported upon.

The purpose of this Standard is to:

(a) Provide a common terminology on Internal Controls to prevent ambiguity or confusion on the subject matter;

(b) Define Internal Controls, how they mitigate risks, and also how they are viewed from a legal perspective;

(c) Explain the responsibilities of management and auditors with regard to Internal Controls, as mandated by law and regulations; and

(d) Specify certain requirements which need to be met to be able to provide an independent assurance on Internal Controls in the organisation under review.

The overall objective of this Standard is to clarify the responsibilities of management and auditors over Internal Controls and how certain requirements need to be met to assess, evaluate, report and provide an independent assurance over Internal Controls.

200 Series: Standards on Internal Audit Management

Standard on Internal Audit (SIA) 210- Managing the Internal Audit Function

The objectives of this Standard on Managing the Internal Audit Function are to ensure the following:

(a) The achievement of overall objectives of internal audit (as outlined in the Internal Audit Charter or Engagement Letter).

(b) Adequate skilled resources and expertise are in place and deployed well, to provide the required level of assurance.

(c) Internal audit assignments are undertaken in a systematic, disciplined and professional manner.

(d) Quality of the work performed forms a sound basis for reporting and is supported by evidence and documentation.

(e) Work is conducted in conformance with the Standards on Internal Audit and other related pronouncements issued by the ICAI.

Standard on Internal Audit (SIA) 220- Conducting Overall Internal Audit Planning

The objectives of an Overall Internal Audit (Engagement) Plan are to:

(a) ensure that the planned internal audits are in line with the objectives of the internal audit function, as per the internal audit charter of the entity (and terms of engagement, where it is an outsourced engagement) and also in line with the overall objectives of the organisation.

(b) align the organisation's risk assessment with the effectiveness of the risk mitigation implemented through internal controls.

(c) confirm and agree with those charged with governance the broad scope, methodology and depth of coverage of the internal audit work to be undertaken in the defined time-period.

(d) ensure that overall resources are adequate, skilled and deployed with focus in areas of importance, complexity and sensitivity.

(e) ensure that the audits undertaken conform at all times with the applicable pronouncements of the Institute of Chartered Accountants of India.

Standard on Internal Audit (SIA) 230- Objectives of Internal Audit

The purpose of defining the Objectives of Internal Audit are to:

(a) Document the formation and functioning of the Internal Audit activity and the terms of the out-sourced internal audit arrangement;

(b) Provide clarity to the Internal Auditor and its stakeholders regarding the nature of the internal audit set-up and its working;

(c) Ensure linkage between what is expected of the Internal Auditor and how those expectation can be met within the Framework governing Internal Audits; and

(d) Promote better understanding on key operational areas, such as, accountability and authority, roles and responsibility, and such other functional matters.

The Objectives of Internal Audit and other terms of engagement of the external service provider are documented in a formal agreement referred to as the Engagement Letter. The Engagement Letter is signed by the Engagement Partner along with the appointing authority of the Company. An indicative list of terms of engagement, covered in an Engagement Letter is provided in this SIA.

Standard on Internal Audit (SIA) 240- Using the Work of an Expert

The overall objective of using the work of an Expert is to allow the Internal Auditor to place reliance on the technical work completed in the most informed manner so as to form an opinion on the outcome of the audit procedures and to add further credibility and reliability to the findings of the internal audit.

Where the findings of the Expert will form part of the assurance report to be issued by the Internal Auditor, the Internal Auditor shall participate in defining the scope, approach, and work to be conducted by the Expert. Otherwise, the Internal Auditor shall not incorporate the finding of the Expert in his Internal Audit report.

300–400 Series: Standards on the Conduct of Audit Assignments

Standard on Internal Audit (SIA) 310- Planning the Internal Audit Assignment

The purpose of defining the Planning the Internal Audit Assignment are to:

a. Ensure its alignment with the objectives of the Overall Internal Audit (Engagement) Plan and in line with stakeholder expectations.

b. Ensure that the scope, coverage, and methodology of the audit procedures will form a sound basis for providing reasonable assurance.

c. Allocate adequate time and resources to important aspects of the assignment and assign appropriate skills to complex areas and issues.

Standard on Internal Audit (SIA) 320- Internal Audit Evidence

The overall objective of obtaining appropriate and reliable evidence is to allow the Internal Auditor to form an opinion on the outcome of the audit procedures completed.

All audit evidence shall be recorded in such a manner that it can be reproduced (if in digital form) and reviewed independently of the Internal Auditor. Details of these quality standards, the manner in which audit evidence shall be gathered, reviewed for sufficiency and appropriateness, validated for authenticity and reliability and stored as part of internal audit documentation, shall be written in the form of an internal audit process (as part of the Internal Audit Manual).

Standard on Internal Audit (SIA) 330 - Internal Audit Documentation

The overall objective of preparing audit documentation is to allow the internal auditor to form an opinion on the outcome of the assignment. The internal audit documentation must stand on its own and not require any follow-up clarifications or additional information to arrive at the same conclusions.

The ownership and custody of the internal audit work papers shall remain with the Internal Auditor. – The internal audit work paper files shall be completed prior to the issuance of the final internal audit report. Any pending administrative matters shall also be completed within sixty days of the release of the final report.

Standard on Internal Audit (SIA) 350 - Review and Supervision of Audit Assignments

The overall objective of review and supervision of an audit assignment is to ensure the effective and efficient performance of the audit procedures in line with quality standards and to accomplish the objectives of the audit.

a. The periodicity and extent of the review shall be planned and documented at the audit planning stage considering the overall audit objectives, time, and budget constraints, as per the professional judgement of the Chief Internal Auditor or Engagement Partner.

b. The documentation shall record the evidence of the supervision and review conducted, including the performance of any audit procedures subsequent to the review.

Standard on Internal Audit (SIA) 360- Communication with Management

The objectives of this Standard to ensure the following:

(a) There is clarity and consensus between the Internal Auditor and the management with regard to the scope, approach, objectives and timing of an internal audit.

(b) To help inform, persuade and act on matters important to the conduct of an internal audit by promoting a continuous dialogue and free flow of information between the Internal Auditor and management.

(c) To help resolve any conflicts in a timely manner.

It explains the importance of two-way communication, both while managing IA function & while conducting an IA assignment. The Internal Auditor shall establish a written communication process and protocol with management including essential exchange of information, cross reference to the internal audit program, where appropriate, and the same is shared and agreed with them.

Standard on Internal Audit (SIA) 370- Reporting Results

On completion of work, IA shall issue a clear, well documented Internal audit report which includes following key elements,

a. Overview of objective, scope, and approach of the audit assignment,

b. The fact that an internal audit has been conducted in accordance the Standards of Internal Audit,

c. An executive summary of key observations covering all important aspects, and specific to the scope of the assignment,

d. A summary of the corrective actions required (or agreed by management) for each observation,

e. Nature of assurance, if any, which can be derived from the observations.

Standard on Internal Audit (SIA) 390- Monitoring and Reporting of Prior Audit Issues

The specific objectives of this standard are to ensure:

a. Proper monitoring and closure of open issues from prior audits.

b. Independent validation of corrective actions taken by the auditee.

c. Escalation of any concerns in case of delays in closure of issues.

d. Timely reporting of status to those charged with governance.

The overall objective of this Standard is to ensure that the auditee mitigate the risks highlighted in the audit observations through timely corrective actions or that a conscious decision is taken to accept the risks, in case recommendations are delayed or not implemented.

500 Series: Standards on Specialised Areas

Standard on Internal Audit (SIA) 520 - Internal Auditing in an Information Technology Environment

The objectives of this standard are to define the essential requirements for auditing in an IT environment so that:

a. Audits are undertaken after due study and understanding of the Organisation's ITE, including the IT strategy, operating procedures, the risk and governance mechanism in place to manage the ITE;

b. An independent risk assessment, along with an evaluation of the controls required to mitigate those risks, forms the basis of the audit procedures; and

c. The audit procedures designed and executed are sufficient to allow an independent assurance, especially in the areas of (indicative list):

- Security and reliability of information.
- Efficiency and effectiveness of information processing.

- Analysis and reporting of the information.
- Continuous access and availability of the information.
- Compliance of the ITE with laws and regulations.

The overall objective of performing internal audits in an ITE is provide independent assurance and help make improvements in the ITE, thus enabling the achievement of business objectives.

Standard on Internal Audit (SIA) 530 - Third Party Service Provider (TPSP)

The primary objective of this standard is to outline the key requirement for providing independent assurance over information residing with third party service providers. These requirements are in the nature of:

a. Assessment of risks associated with securing and protecting the information;

b. Evaluation of adequacy of controls to address risk of errors and irregularities from financial, operational processing and reporting requirements;

c. Cost and operational efficiencies in the collection, storage and processing of company information; and

d. Ensuring compliance with IT policies and standards, as well as contractual, statutory, and regulatory requirements.

One objective is to issue an independent audit report on TPSP's Controls. These reports are designed to help the User Entity to build trust on the controls at the TPSP. Conversely, these reports also help to build confidence with the TPSP in their own service delivery processes and controls.

Another objective of this standard is to outline requirement of the Internal Auditor in evaluating the TPAA report provided by Independent auditor covering outsourced processes of TPSP.

INTERNATIONAL STANDARDS BY INSTITUTE OF INTERNAL AUDITORS (IIA)

Now that we have discussed the national standards, let us also have a look at the international standards defined by the IIA. IIA stands for the Institute of Internal Auditors, headquartered in USA, which is an international professional association of internal auditors. IIA has established a set of standards that provide guidance and best practices for internal auditing. These standards are known as the International Standards for the Professional Practice of Internal Auditing (or IIA standards).

The IIA standards are divided into three categories:

1. **Attribute Standards:** These standards deal with the characteristics of organizations and individuals performing internal auditing. They cover areas such as independence, objectivity, and proficiency.
2. **Performance Standards:** These standards deal with the nature of internal auditing work and how it should be performed. They cover areas such as planning, execution, reporting, and follow-up.
3. **Implementation Standards:** These standards provide guidance on how to implement the attribute and performance standards. They cover areas such as quality assurance and improvement programs, governance, risk management, and control processes.

The IIA standards provide a framework for internal auditors to carry out their work in a professional and effective manner. They help to ensure that internal audit activities are performed with integrity, objectivity, and due professional care. Compliance with the IIA standards is also a key factor in ensuring that internal audit activities meet the expectations of stakeholders, such as management and external auditors.

A quick snapshot of IIA standards is given below:

International Standards for the Professional Practice of Internal Auditing (Standards) - Issued by The Institute of Internal Auditors, USA

- Attribute Standards
  - 1000 – Purpose, Authority, and Responsibility
  - 1010 – Recognizing Mandatory Guidance in the Internal Audit Charter
  - 1100 – Independence and Objectivity
  - 1110 – Organizational Independence
  - 1111 – Direct Interaction with the Board
  - 1112 – Chief Audit Executive Roles Beyond Internal Auditing
  - 1120 – Individual Objectivity
  - 1130 – Impairment to Independence or Objectivity
  - 1200 – Proficiency and Due Professional Care
  - 1210 – Proficiency
  - 1220 – Due Professional Care
  - 1230 – Continuing Professional Development
  - 1300 – Quality Assurance and Improvement Program
  - 1310 – Requirements of the Quality Assurance and Improvement Program
  - 1311 – Internal Assessments
  - 1312 – External Assessments
  - 1320 – Reporting on the Quality Assurance and Improvement Program
  - 1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"
  - 1322 – Disclosure of Nonconformance
- Performance Standards
  - 2000 – Managing the Internal Audit Activity
  - 2010 – Planning
  - 2020 – Communication and Approval
  - 2030 – Resource Management
  - 2040 – Policies and Procedures
  - 2050 – Coordination and Reliance
  - 2060 – Reporting to Senior Management and the Board
  - 2070 – External Service Provider and Organizational Responsibility for Internal Auditing

- 2100 – Nature of Work
- 2110 – Governance
- 2120 – Risk Management
- 2130 – Control
- 2200 – Engagement Planning
- 2201 – Planning Considerations
- 2210 – Engagement Objectives
- 2220 – Engagement Scope
- 2230 – Engagement Resource Allocation
- 2240 – Engagement Work Program
- 2300 – Performing the Engagement
- 2310 – Identifying Information
- 2320 – Analysis and Evaluation
- 2330 – Documenting Information
- 2340 – Engagement Supervision
- 2400 – Communicating Results
- 2410 – Criteria for Communicating
- 2420 – Quality of Communications
- 2421 – Errors and Omissions
- 2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"
- 2431 – Engagement Disclosure of Nonconformance
- 2440 – Disseminating Results
- 2450 – Overall Opinions
- 2500 – Monitoring Progress
- 2600 – Communicating the Acceptance of Risks

- Implementation Guidance
  - Guide for IIA Code of Ethics
  - Guide for each of the standards

Latest version of IIA standards can be downloaded from the website of IIA by its members

While ICAI & IIA aim to improve the quality and effectiveness of internal audits, there are some differences between the standards they set. The ICAI sets out guidelines for its members who may be working in India or any other country. The latest revised standards cover most of the contemporary issues faced by the internal audit professionals.

On the other hand, IIA standards are more globally recognised. These standards have been made keeping the global issues and challenges faced by internal audit profession and may not be able to cater to the specific local regulations in all matters. Yet, they are comprehensive and widely respected.

While choosing to adopt a particular set of standards, the audit committee or the board may consider the relevance of operations of the company, perception of relevant stakeholders, and the opinion of the internal auditor. For instance, the board of a multi-national company headquartered in USA, and having its operations in India shall be more willing to adopt the IIA standards instead of SIAs. On the other hand, a company head quartered in India having international operations may like to adopt SIAs, being the standards which are more aligned to the regulations in India. The past experiences and perception of board members as well as internal auditor may also impact this decision.

INTERNAL AUDIT PRACTICES

Internal Audit Manual

While the fundamental principles for internal audit activity are detailed in the standards, we need to imbibe the same in the day-to-day operations of a company by translating the requirements into the policies and procedures related to internal audit activity. Putting in place an internal audit manual is a good practice which is followed by most organisations.

A typical internal audit manual has below given contents:

- Definition of internal audit as adopted by audit committee / board (e.g., SIAs or IIA)
- Scope, objectives, and any exclusions from internal audit activity
- Reporting and Review responsibility (functional and administrative)
- Authority
- Rules of conduct / Code of Ethics
- Procedural aspects
    - Planning and approval
    - Audit Universe
    - Audit Planning Methodology
    - Frequency of Internal Audits
    - Engagement Planning
    - Audit Performance process (audit notifications, kick off meetings, working paper requirements, audit records, draft report and final report circulation etc.)
    - Monitoring Progress
    - Categorization of Audit Findings

This document needs to be drawn out clearly in line with the standards adopted by the company, and then reviewed and approved by the audit committee or the board. While an extract of internal audit manual defining all the aspects except the procedural parts (usually known as Internal Audit Charter) is normally made available to all the employees of the organisation on mediums such as Intranet of the company, the detailed internal audit manual containing procedural part is usually made available to all the members of the internal audit team. The internal auditor should seek guidance from the board or audit committee about circulation of these documents.

In case there is no internal auditor on the rolls of the company, the external firm appointed by the board or audit committee may make such a manual and get it approved from the board or audit committee. The auditor

so appointed may decide the circulation of such manual to relevant stakeholders, as per the directions of the board or audit committee.

Further, documentation of any exclusions to the scope of internal audit activity is important for the audit committee or boards. Thus, the same should be clearly brought out in the internal audit manual. For instance, in some companies the management audits are done by a separate department, and in such case, it is important to put these audits as an exclusion in internal audit manual. Similarly, the health and safety audits, secretarial audits, statutory audits, and ISO audits may or may not be under the scope of internal audit and thus a clarity on the same should be brought out in the internal audit manual. In the absence of such exclusions, the internal auditor may be perceived to be responsible for such activities as well.

CORPORATE SOCIAL RESPONSIBILITY

Corporate Social Responsibility is the way companies manage their businesses to produce an overall positive impact on society through economic, environmental and social actions. Corporate social responsibility (CSR), also called corporate conscience, corporate citizenship, social performance, or sustainable responsible business/ businesses. Business depends for its survival on long term prosperity of the society

CSR has been defined by different people giving it a varied dimension. According to Michel Hopkins "Corporate Social Responsibility is concerned with treating the stakeholders of a company or institution ethically or in a responsible manner. 'Ethically or in a responsible manner' refers to treating key stakeholders in a manner deemed acceptable according to international norms."

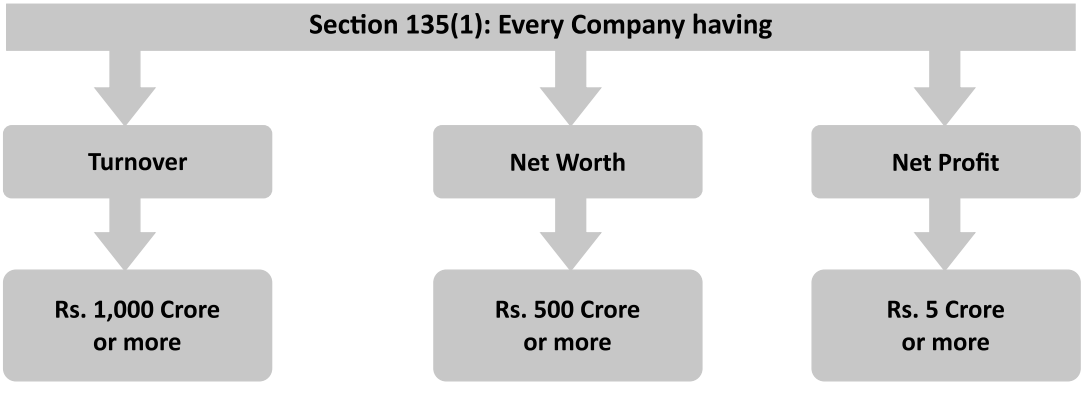
Corporate social responsibility is basically a new business strategy to reduce investment risks and maximise profits by taking all the key stakeholders into confidence. The proponents of this perspective often include corporate social responsibility in their advertising and social marketing initiatives. It is a tool to increase the reputation of the company in the eyes of society.

The concept of Corporate Social Responsibility was introduced in India within legal framework by the Companies Act, 2013.

Applicability under Companies Act, 2013

Section 135 (1) read with rule 3 of Companies (Corporate Social Responsibility Policy) Rules, 2014, mandates that every company which fulfils any of the following criteria during the immediate preceding financial years shall constitute a CSR Committee –

- Companies having net worth of rupees five hundred crore or more, or
- Companies having turnover of rupees one thousand crore or more, or
- Companies having a net profit of rupees five crore or more



Illustrative Checklist for Corporate Social Responsibility provisions under Companies Act, 2013

1. Check if the constitution of CSR Committee is applicable to company.
2. If yes, whether the company has constituted CSR committee of the board consisting of three or more directors, out of which at least one director is an independent director.

   In case where a company is not required to appoint an independent director under sub-section (4) of 149, it shall have in its CSR Committee two or more directors.
3. Whether the company has CSR policy approved by the CSR Committee.
4. Whether the CSR committee has recommended list of CSR projects or programme within the purview of schedule VII.
5. Whether the monitoring process of such projects or programme has been established by the company.
6. The composition of CSR committee is disclosed in the board's report.
7. Check whether the CSR activities were under taken as per CSR policy and projects, programs or activities excludes activities undertaken in pursuance of its normal course of business.
8. Corporate social responsibility committee has recommended the amount of expenditure to be incurred on the activities referred in the Corporate Social Responsibility policy.
9. The company has instituted a transparent monitoring mechanism for implementation of the CSR projects or programs or activities undertaken by the company.
10. The company has disclosed the contents of the policy in board's report and at its website, if any.
11. The board's report includes an annual report on CSR containing prescribed particulars.
12. In case the company does not spend the specified amount (i.e. at least two percent of the average net profits made during the three immediately preceding financial years), Board's report specifies the reason for not spending the amount.
13. Check if the net profits of the company are in accordance with the provisions section 198 of the Companies Act, 2013 or not.
14. In case the company has built CSR capacities of their own personnel, check whether the expenditure including expenditure on administrative overheads shall not exceed five percent of total CSR expenditure of the company in one financial year.
15. The company has complied with all other requirement of the CSR Rules.

Role of Internal Auditor in Corporate Governance

An effective internal audit function can play a significant role within the corporate governance framework of a company. Over the last decade, internal audit has developed and grown in importance. Efficient internal audit functions provide objective assurance/assessments to the board (and to the audit committee) about the adequacy and effectiveness of the processes by which risks are identified and prioritised; managed, controlled, and mitigated. In most countries and business sectors internal audit reports professionally to an audit committee and managerially to the chief executive or chief financial officer. Internal audit is an independent and objective appraisal function; it supports senior management and the (management) board. Internal audit activities are performed in diverse legal and cultural environments; within organisations that vary in size and structure. Internal audit functions should comply with the relevant professional standards.

CODE OF ETHICS

The primary purpose of a code of ethical conduct for a professional organisation is to promote an ethical culture among professionals who serve others. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management and control.

A code of ethical conduct worded so as to reduce the likelihood of members being sued for substandard work would not earn the confidence of the public. A code of ethical conduct can help establish minimum standards of competence, but it is impossible to require equality of competence by all members of a profession. To be effective, the code must provide for disciplinary action for violators.

ENVIRONMENTAL AND SOCIETAL SAFEGUARDS

Internal Audit has become an important management tool for the following reasons

1. Internal Auditing is a specialized service to look into the standards of efficiency of business operation.
2. Internal Auditing can evaluate various problems independently in terms of overall management control and suggest improvement.
3. Internal Audit's independent appraisal and review can ensure the reliability and promptness of MIS and the management reporting on the basis of which the top management can take firm decisions.
4. Internal Audit system makes sure the internal control system including accounting control system in an organization is effective.
5. Internal Audit ensures the adequacy, reliability and accuracy of financial and operational data by conducting appraisal and review from an independent angle.
6. Internal Audit is an integral part of "Management by System".
7. Internal Audit can break through the power ego and personality factors and possible conflicts of interest within the organization.
8. It ensures compliance of accounting procedures and accounting policies.
9. Internal Auditor can be of valuable assistance to management in acquiring new business, in promoting new products and in launching new projects for expansion or diversification of business.

CHANGE MANAGEMENT

Organisations are always involved in a variety of change, and this is not just confined to internal projects. For example, it could also encompass interaction with suppliers and customers. The change being undertaken by organizations now is inherently complex and often impacts diverse stakeholder groups both internally and externally. As the change portfolio grows the level of complexity grows with it. With many organizations now find it difficult to understand and track the plethora of change initiatives underway. An added complexity is a reduction in manpower and the availability of skilled resources.

The term change refers to an alteration in a system whether physical, biological or social. Thus organization change is the alternation of work environment in the organization. It implies a new equilibrium between different components of the organization i.e., technology, structural arrangement, job design, and people. An organization change may have following features:

(i) Any change may effect the whole organization;

(ii) When change occurs in any part of the organization, it disturbs the old equilibrium necessitating development of a new equilibrium;

(iii) Organization change is a continuous process.

LESSON ROUND-UP

- There are several laws and regulations that govern internal audit related activities in India. Some of the key laws applicable to internal audit in India are:

    1. **Companies Act, 2013**: Section 138 of the Companies Act, 2013 mandates that certain classes of companies shall appoint an internal auditor who shall conduct an internal audit of the functions and activities of the company. These requirements are defined in Rule 13 of the Companies (Accounts) Rules, 2014.
    2. **Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements), Regulations 2015**: These regulations define requirements for listed companies' audit committee and their interaction with internal audit activity. They cover amongst others, reporting of internal audit, specific items to be reviewed in relation to internal audit, and audit committee interactions with internal auditors.
    3. **Reserve Bank of India (RBI) Guidelines**: The RBI has issued guidance note on Risk Based Internal Audit for various entities such as banks, non-banking financial companies (NBFCs), and payment system providers. These guidelines were amended in January 2021 and their applicability was extended to NBFCs, and UCBs also in February 2021.
    4. **Insurance Regulatory and Development Authority of India (IRDAI)** regulations has issued Guidelines for Corporate Governance for Insurers in India in 2009, which have been updated in 2016. These guidelines define the requirements for Board to lay down policy framework for control functions such as internal audit department, audit committee oversight on internal audit activity, and responsibilities of internal auditors.

- There are two standards that are widely used by companies in India:

    1. Standards on Internal Audit (SIAs), issued by Institute of Chartered Accountants of India
    2. International Standards for the professional practice of Internal Auditing, issued by the Institute of Internal Auditors, USA.

- Both these standards are based on similar principles about the concept of internal auditing. However, there are aspects which can be different from each other. Thus, an internal auditor needs to understand these standards well before making a proposal to adopt any of them by the audit committee or board.
- **SIAs are principle based** and clearly outline the objective of issuing the Standard along with the essential requirements for its compliance. Internal Auditors shall apply their best professional judgement in the implementation of SIAs on a "substance over form" basis.
- The Governing Framework of SIAs defines the basic principles of Internal Audit, which is a set of core principles fundamental to the function and activity of internal audit. The Basic Principles are critical to achieve the desired objectives as set out in the Definition of the Internal Audit, and therefore, apply to all internal audits.

- The IIA standards are divided into three categories:
  1. Attribute Standards: These standards deal with the characteristics of organizations and individuals performing internal auditing. They cover areas such as independence, objectivity, and proficiency.
  2. Performance Standards: These standards deal with the nature of internal auditing work and how it should be performed. They cover areas such as planning, execution, reporting, and follow-up.
  3. Implementation Standards: These standards provide guidance on how to implement the attribute and performance standards. They cover areas such as quality assurance and improvement programs, governance, risk management, and control processes.
- The primary purpose of a code of ethical conduct for a professional organisation is to promote an ethical culture among professionals who serve others. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management and control.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. Briefly explain the provisions of Companies Act, 2013 governing Internal Audit?
2. Explain briefly the clause stated in CARO 2020 relating to Internal Audit.
3. What are the role of Audit Committee in terms of evaluation of Internal Financial Controls (IFC)?
4. What are the Basic Principles governing Internal Audit?
5. Briefly explain the Governing Framework of Standard of Internal Audit (SIA).
6. How do you define the term “Independence” with respect to carry out Internal Audit Function?
7. What do you mean by the term “Due Professional Care”?
8. State the Skill & Competence required by the Internal Auditor?
9. Explain the SIA 310 relating to planning the Internal Audit?
10. Briefly narrate the SIA 240 relating to using the work of an Expert.
11. Explain the SIA 330 which talks about Internal Audit Documentation?
12. Short Note on -

    SIA 390 - Monitoring and Reporting of Prior Audit Issues

    SIA 370 - Reporting Results

    SIA 530 - Third Party Service Provider

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's

- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Internal Controls

Lesson 3

KEY CONCEPTS

■ Internal Control ■ Internal Check ■ Preventive Control ■ Detective Control ■ Input Control ■ Output Control ■ Risk Management

Learning Objectives

To understand:

- The meaning & definition of Internal Control
- Objectives, dimensions and types of Internal Control
- What are the Difference between Internal Check and Internal Control
- What are the benefits and limitation of Internal Control
- The various internal control techniques
- Internal control frameworks prescribed by COSO, Cadbury committee
- Role of internal auditors in implementation of internal controls
- How to examine the effectiveness and efficiency of internal controls
- Fraud risk awareness
- Risk Management, Types of Risks, Enterprise Risk Management, Risk Management Plan
- Recommend internal controls to prevent and detect fraud and educate to improve the organisation's fraud awareness
- What are the role of Internal Control in the New Digital ERA such as Robotic Process Automation (RPA), Artificial Intelligence and Machine Learning, Block chain Technologies, Cloud Computing

Lesson Outline

- Background
- Meaning and Definition of Internal Control
- Objectives of Internal Control
- Dimensions of Internal Control
- Types of Controls (Preventive, detective, input, output)
- Internal Audit and Internal Controls
- Benefits and Limitation of Internal Controls
- Internal Control Techniques
- Internal Control Frameworks (COSO, Cadbury)
- Role of Internal Auditors in Implementation of Internal Controls
- Examine the effectiveness and efficiency of internal controls
- Fraud Risk Awareness
- Risk Management
- Recommend controls to prevent and detect fraud and educate to improve the organization's fraud awareness
- Role of Internal Control in the New Digital ERA
- Practice Questions
- Lesson Round-Up
- Test Yourself
- List of Further Readings

BACKGROUND

To understand the internal controls, it is important to understand the relationship which exists between the directors or those charged with governance (TCWG), the members (or shareholders) of a corporate entity be it a private company or a public company or Section 8 company of the Companies Act, 2013 ("the Act") and the auditors (statutory and internal) for it is relevant to the object and significance of an audit of such a company.

A company is in law regarded as a separate legal entity independent from its members. (Salomon v Salomon & Co. Ltd. (1897). However it has no physical existence, neither soul nor a body of its own. The company itself cannot act in its own person, it can only act through directors. The board of directors are the brain of the company and the company can and does act only through them.

In view of the above, the directors of the company are appointed by the members to manage their company and the Act has set out their responsibilities for ensuring that the company keeps proper financial and non-financial records and for presenting audited annual accounts to the members.

However, in practice the day to day running of the company and the work of keeping and maintaining appropriate financial and non-financial records commensurate with the size and nature of business is often delegated by the directors to the employees.

The directors can discharge their responsibilities by instituting adequate internal controls and internal checks to ensure that this work is carried out properly by the employees. The directors can then rely on this system for the production of reliable management information, financial records, cost accounting records etc. and to prevent errors, frauds and loss of the company's assets.

The responsibility for safeguarding an organization's assets, maintaining proper records and preventing and detecting errors and frauds rests with the directors or those charged with governance. The members or other stakeholders must look to the directors or those charged with governance and not the auditors for the effective discharge of this duty.

As per the provisions of the Act, the board of directors may delegate certain of their responsibilities relating to maintenance of financial and non-financial records and systems of internal controls, review of interim financial statements and annual financial statements to an "audit committee". Audit committee may comprise of both executive and non-executive directors as prescribed under the Act in according to size and nature of its business.

Even in the case of non-corporate entities, not-for-profit organisations, internal control plays a vital role in running a sustainable enterprise.

MEANING OF INTERNAL CONTROL

Internal controls are the mechanisms, rules and procedures implemented by an entity to ensure the integrity and reliability of financial and non-financial records, management information and cost accounting records, promote accountability, prevent and detect errors and frauds. The auditors also rely on the system of internal control for the purpose of audit of the financial accounts.

Internal control comprise internal accounting controls and operational controls. The auditors are primarily concerned with internal accounting controls.

Basic controls include features like control accounts and numerical controls to ensure that all transactions are completely accounted for in the books of account. Disciplines over basic controls include the segregation of incompatible duties, segregation of custody of assets from the accounting responsibilities, physical safeguards to prevent unauthorised access to assets or accounting and other sensitive records and internal check.

DEFINITIONS OF INTERNAL CONTROL

As per Section 134 of the Companies Act, 2013, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring, orderly and efficient conduct of business, including

adherence to company's policies, safeguarding of its assets, prevention and detection of frauds and errors, accuracy and completeness of the accounting records, and timely preparation of reliable financial information.

Committee of Sponsoring Organizations of the Treadway Commission **(COSO)** defines internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

The Institute of' Chartered Accountants of England and Wales defines Internal Control as "Internal Control means not only internal check or internal audit, but the whole system of control, financial and otherwise, established by management in order to carry on the business of the company in an orderly manner, safeguard its assets and secure as far as possible accuracy and reliability of its records".

De Paula defines, "internal control as system of controls, financial and otherwise, established by management in order to carry on the business of the company in an orderly and efficient manner, safeguard the assets, secure as much as possible the completeness of an internal control system".

Definition as per International Standard on Auditing 315

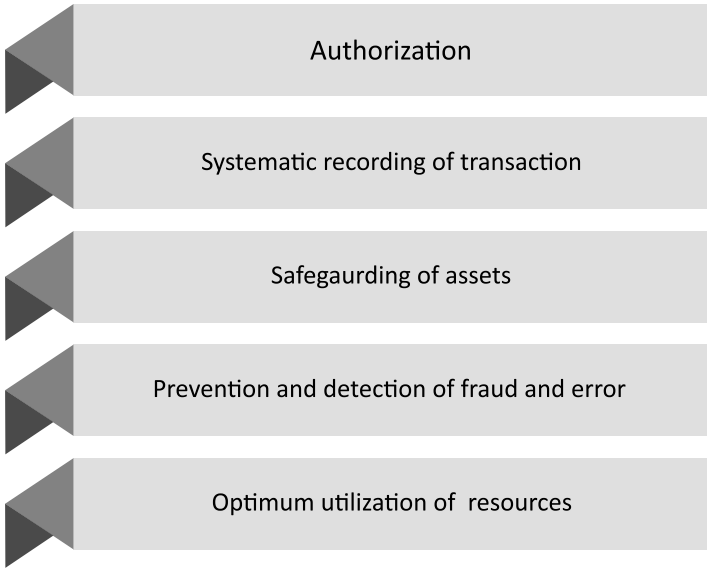
Internal Audit as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations". The term "controls" refers to any aspects of one or more of the components of internal control.

Definition of control as per the Institute of Internal Auditors, USA (IIA)

Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Gibbins, [1990]; argues that internal controls may be incorporated with in computerized accounting system, which extends beyond those matters which are related directly to the accounting system.

OBJECTIVES OF INTERNAL CONTROL



- To ensure that the business transaction takes place as per the general and specific authorisation of the management. Ensuring all the authorised transactions are recorded in the financial and non-financial records.
- To ensure that there is a systematic recording of every transaction completely, sequentially with the accurate amount in their respective account and in the correct accounting periods in which they occur as per generally accepted accounting principles and accounting standards.
- To safeguard the entity's assets from unauthorised use with the help of physical security systems, anti-theft devices like RFID, burglar alarms and cameras etc.
- To compare the assets both current and non-current as per the records with that of the physical assets at regular intervals and report to TCWG, in case any difference is found.
- To review the working of the organization and the loopholes in the operations and take necessary steps for its correction.
- To ensure there is the optimum utilization of the entity's resources.
- To find out whether the financial statements are in alignment with the accounting standards and generally accepted accounting principles.

Players in the Internal Control Frameworks

Accounting and Finance Department, Internal audit professionals are the key players along with the other departments in the internal control frameworks of their entity. In today's rapidly changing, technologically disruptive world with artificial intelligence, robotic process automation, machine learning etc., entities across the world face many challenges grappling with Big Data. Data-driven insights enable management to act and react quickly and take decisions as appropriate.

With a strong commitment to trust and ethics effective internal control system require a combination of people, process and technology and data driven entity.

DIMENSIONS OF INTERNAL CONTROL

As per Foreign Corrupt Practices Act, 1977 of United States of America, accounting provisions require issuers (both U.S. and non-U.S. companies that are publicly traded in the United States) are required to establish and maintain a system of internal controls sufficient to assure that

(i) transactions are executed in accordance with management's authorization;

(ii) access to assets is permitted only with the proper authorization; and

(iii) the accounting records reflect the existing assets.

Later in the year 1985, COSO began as a private sector initiative to investigate the causal factors that lead to fraudulent financial reporting as a result of a number of accounting scandals that emerged in the 1970s and mid-1980s.

This initiative was termed the National Commission on Fraudulent Financial Reporting. The first president of the Commission was James C. Treadway, Jr., a former Commissioner of the US Securities and Exchange Commission, and therefore the initiative was commonly called the **"Treadway Commission".**

One of the major factors that influences a business organisation to adopt internal control is to provide a reliable financial statements to its stakeholders especially in this start-up era.

CASE STUDY

A firm with two partners who take active part in running the vegetable business, with two assistants. The firm has a simple accounting system and does not need more than a cash and bank book to record. Expenses such as rent and insurance, Purchase of vegetables like cabbages, carrot, potatoes, onion etc. Sale of vegetables etc.

The expenses and purchases are supported by two box files of "paid" and "unpaid invoices" and they have billing machine to record sales.

As an internal auditor how would you ensure that sales and purchases were completely and accurately recorded?

Solution:

The following controls would be helpful in ensuring that sales and purchases were fully and accurately recorded by the company in vegetable selling business.

Purchases

1. Since some of the vegetables have limited shelf life, purchases of stock are to be made by the partners of desired quantity and quality to avoid wastages.
2. Invoices to be numbered on receipt of goods to ensure that all purchase invoices are filed in the invoice files. This control is backed up by periodic sequence checks.

   [A sequence check is a check to ensure that a sequence of numbers is complete. For example if purchase invoices in the file contains 1,2,3,5 and 6, invoice number 4 can be seen as missing and steps shall be taken to recover it.]

Sales

1. Personal supervision of the two assistants by the partners, at least one partner has to be in the shop during opening and closing hours since most frauds are perpetrated at this time.
2. Comparison by the directors of actual sales with expected sales on a weekly basis.
3. Comparison of actual and expected gross margin on a monthly basis.

Accounting controls: The basic accounting system and such controls as the use of accounting information to detect variances from expectation (comparing of actual sales with expected sales) and those that ensures that records are complete using sequence checks.

Administrative controls: Non-accounting controls such as the personal supervision by the partners and restriction of purchasing to the partners.

Consider the way in which purchase invoices are numbered and filed. The numbering makes it more likely that all transactions have been recorded, the sequence check strengthens this control and also aids detection of errors and/or frauds. Considering the size of business, segregating of purchase invoices in two different files as paid and unpaid enables outstanding creditors to be easily established.

Safeguarding of assets : An important control in the vegetable shop to safeguard the assets (cash and vegetable stock which are highly susceptible to theft) is that of close supervision by the partners.

Partners personally purchase the produce to be sold, this control is to ensure that management policy of selling a particular grade of vegetables is being adhered to.

The carrying on of the business in an efficient and orderly manner can be exemplified by the use of accounting information to enable the partners set the prices of the vegetables.

A proper record of purchase cost of vegetables would be a prerequisite for setting sale price.

Difference between Internal Check and Internal Control

Internal Check can be defined as a method or an arrangement of the operations of a factory, office, warehouse, store, etc, in a manner that the work of one employee automatically comes under the scrutiny of another employee, so as to minimize the risk of errors and frauds.

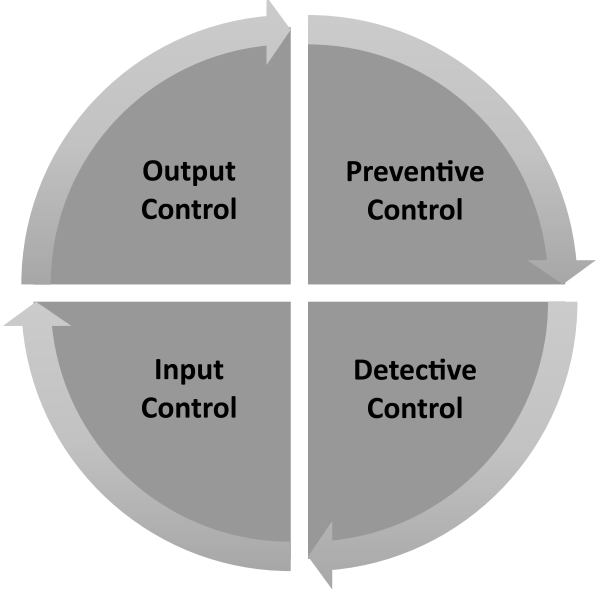
Internal Check	*Internal Control*
It is a method of arranging the operations of an enterprise wherein the work of one employee is automatically checked by another employee to minimise the risk of error and fraud.	It is a whole system of controls financial and otherwise established by the management.
Scope of internal check is very limited and in the case of small enterprises it is practically difficult.	Scope of internal control is very wide, it includes internal check and internal audit.

TYPES OF CONTROL

There are preventive, detective, physical and logical controls in all entities commensurate with its size and nature of its business.

Examples of internal controls are internal audits, firewall deployment, training, and employee disciplinary procedures. All organisations are subject to various risks that might harm the organization and could result in asset loss, reputation loss and so forth. From unintentional mistakes to fraudulent manipulation, risks are present in every business.

The importance of internal controls lies in their ability to protect the organization from risks and the consequences thereof. For example, IT security controls reduces the risk of data breaches or malware infection. It helps to find weak spots in information systems and then strengthen those weak spots. Internal controls have its limitation on what it can accomplish; hence it is essential to have an ongoing reviews and monitoring of existing internal control system.



1. Preventive Control

We have heard many times that "prevention is better than cure". Preventive internal controls are put in place to prevent an adverse event from occurring. For example, many software applications have built-in checks and balances to avoid entering incorrect information.

Preventive controls are the best kind of controls because they lessen the need to detect errors and fraud after it has occurred. Automated preventative controls are even better because they remove the need for human intervention. They are proactive in nature that assists the management to ensure that strategic and departmental objectives are achieved.

Examples of Preventive Internal Controls

Segregation of duties, Rotation of duties, background verification of employees, prior approvals, authorisation and verification, firewalls, computer and server backups are all preventive internal controls that block undesirable events from occurring.

Background screening for employees:

Background screening is a procedure where employers check candidates' backgrounds, screen them for drugs, check references, and assess their conduct. It is used in the recruiting process to screen out many undesirable candidates before investing in the onboarding process. Many a frauds can be prevented by this process.

2. Detective Controls

Detective internal controls detect an error or fraud after it has occurred. Ideally, detective internal controls will discover an issue before it becomes a significant problem. It is more of a post mortem exercise.

Examples of detective controls are internal audits, reconciliations, financial reporting, financial statements, and physical verification.

3. Input Controls

Input controls in the context of internal control means the procedures and systems to ensure completeness, accuracy, existence, validity of the data entered in the financial and non- financial records. Input control helps in preventing errors and frauds thereby making the information is reliable for decision making.

Examples are: Data validation, Data verification, Audit trail and authorisation procedure.

4. Output Controls

Output controls in the context of internal control means the mechanism put in place to monitor and evaluate the results of operation or activities. The purpose of output control is to ensure that the objectives of the entity are met and the results are in line with the expectations.

Examples are: Monitoring and measuring key performance indicators such as productivity, efficiency and effectiveness, quality control, obtaining feedback, review of exception reports.

INTERNAL AUDIT & INTERNAL CONTROLS

The objective of an internal audit is to evaluate compliance with company procedures, applicable laws, and international standards. Data and reports are reviewed to assure consistency and compliance. This internal control provides a value-added service to management and to the board of directors by detecting and correcting weaknesses in a process before external audits discover them. This can protect the organisation from loss of reputation and regulatory fines.

1. **Periodical reconciliations and financial reporting:** Reconciliations are performed to verify financial reporting among various sources. For example, comparing (or reconciling) a bank statement or debtors statement of account to a company's internal records is one form of reconciliation.

   Financial reporting discloses the entity's revenues, expenses, cash flow, and financial health. It allows executives and investors to make more informed judgments on performance and opportunities for improvement. Unusual or unexpected variances in financial statements helps to detect inadvertent errors and intentional fraud.

2. **Physical verification:** Physical verification of tangible assets is performed periodically to assure actual count of assets (inventory, property, plant and equipment, investments, cash etc) match what is recorded in business systems and financial statements. Physical assets values directly affect the balance sheet, so it's vital they are reflected accurately. Discrepancy investigations can reveal system issues, inadvertent errors, and possibly embezzlement or theft. This is helpful at remote locations like branches, manufacturing facilities, warehouses, projects.

3. **Corrective Internal Controls:** Corrective internal controls are implemented after the internal detective controls discovers a problem. These controls could include disciplinary action, report filing, software patches or modifications, and new policies. They are usually put into place after a root cause investigation.

   Examples of Corrective Internal Controls

   Corrective internal controls, by nature, are specific to the typical flaws and risks of the company, previously evaluated through comprehensive risk assessments or detective controls, such as audits.

4. **New or Updated Policies and Procedures:** Policies and procedures needs to be updated when an audit or other detective control identifies a gap in processes or if new Enterprise Resources Planning software is implemented. For example, root cause analysis on a physical inventory discrepancy may reveal that employees are inadequately trained on how to account for the parts that fail quality checks. Corrective controls would include updated work instructions and training.

5. **Disciplinary Actions:** Disciplinary actions are corrective actions taken in response to employee misbehavior, rule violations, or poor performance. Discipline can take several forms depending on the seriousness of the situation, including a verbal warning, formal warning, an unfavorable performance evaluation, or even termination.

BENEFITS AND LIMITATIONS OF INTERNAL CONTROLS

Processes and control activities are imperfect, and errors and problems will inevitably be found. Therefore, an ongoing review and analysis of internal controls should be a part of any organization's regular processes.

Benefits of Internal Controls

Management is ultimately responsible for the control environment and the success of internal controls. The benefits of internal controls depend upon correct implementation and ongoing monitoring.

1. **Early Warning System:** Internal controls serve as an early warning system to identify issues before they become big problems. Quality checks prevent faulty products from being shipped to customers. The investigation into a slip in on-time delivery metrics may reveal a more significant problem on the horizon. Problems are easier to fix when you catch them early.

2. **Prevent Fraud:** Robust internal controls deter employees from engaging in misconduct. When employees can see process gaps, they may be tempted to perform minor inappropriate actions that

eventually lead to major ones. With multiple checks and balances, however, fraud is much more difficult. Solid policies assure that employees understand the consequences.

3. **Avoid External Audit Findings and Regulatory Fines:** Performing investigations and corrective actions on external audit findings can be a laborious process. If an external audit identifies a significant gap in processes or material misstatements, entity could be exposed to losing industry certifications or substantial fines. It is always best to find and fix a problem before an external entity discovers it.

   If an entity still experience a data breach, robust internal controls can also protect it from hefty fines. If an investigation reveals that the entity acted with due diligence and had adequate controls in place, a regulatory agency may reduce penalties.

Limitations of Internal Controls

Despite the benefits, internal controls have some limitations. It's crucial to be aware of the gaps left by internal controls to assure that those risks are understood.

1. **Collusion (Override a control):** Segregation of duties is one of the most prevalent internal controls businesses use. It separates tasks so that no one employee has the power to commit fraud. Employees can, however, get past this by collaborating together in an elaborate process to disguise their fraud. Collusion involves two or more employees agreeing to take common action to override a control.

   For example, employee A is the warehouse manager in charge of stock and another employee B from accounts department is required to count stock and compare it with stock records. A misappropriates stock and B is aware of it and helps A by falsely reporting that there are no discrepancies between stock records and physical count. This is a clear case of Collusion.

2. **Human Error:** Human error can be another disadvantage of internal controls, especially when relying on manual processes and judgment calls. For example, inadvertent errors can be made during manual inventory counts, and poor judgment could impact internal audit results. Wherever possible, automated systems should be employed to drive consistency and reduce human error.

   For example, weighing scales along with CCTV cameras can be used in stockrooms to verify inventory counts. Automated systems can help perform reconciliations among accounting and financial records. Solid auditing processes, along with management oversight, will support rigorous internal auditing standards.

3. **Unforeseen Circumstances:** Internal controls rely on a company's management anticipating all potential hazards and implementing mechanisms to prevent or mitigate them. Still, management cannot anticipate all potential challenges or events. Random variables or occurrences are prone to render internal controls ineffective.

   Moreover, attempting to control unusual conditions can be costly, and a management team may instead choose to accept the risk. For example during lockdown time during pandemic employees were working remotely from their home. As a result, internal controls may be limited in their use under unexpected or extraordinary scenarios.

   Apart from risk assessments, procedures, reporting, and communication, the only thing that all internal control schemes have in common is detailed documentation and reporting.

   Small companies may begin by managing their controls with spreadsheets, but the number of internal and external stakeholders increase as their business grows. As a result, preparing ahead of time can save time and money in the long run by having latest version of software appropriate to the size and nature of business.

4. **Internal Controls in Smaller Entities:** Fewer employees limits the extent of segregation of duties but if owner –manager has effective oversight it may compensate to some extent. Overriding of controls by owner-manager is a significant risk because the system of internal control is less structured.

INTERNAL CONTROL TECHNIQUES

1. **Segregation of Duties:** Separation of duties is a critical internal control designed to reduce the incidence of error or fraud by assuring that no single employee has the potential to both perpetrate and hide errors or fraud in the course of his or her activities. Assigning one person to write cheques and another staff member to authorise the payments is one example of segregation of duties. In general, the primary incompatible responsibilities that must be separated are Performing transactions, Authorisation or acceptance, Reconciliation, Asset custody.

2. **Access Controls:** Access controls ensures who has or what has access to corporate assets, including IT systems. These controls are a crucial security concept that reduces risk to the company or organisation. Limiting access to sensitive information and systems only to authorised personnel.

   Physical access control limits access to manufacturing areas, buildings, vital installations, and physical IT assets. Security guards verifying ID credentials or access key cards or biometric access (facial recognition or thumb impression) may be employed to enforce physical access control. Common security measures that prevent physical access in smaller entities are locks, burglar alarms and cameras.

   Physical controls also includes indirect access via documentation. It refers to the fact that the use of inventory needs to be controlled and the inventory should be released only if it is authorised. It will be meaningless to keep inventory in a locked area if anyone can obtain as much as they want without any authorisation.

   Logical access control restricts connections to computer networks, system files, and data. The principle of the least privilege is an information security standard that says users should only access system functions and data that are necessary for the user to do his or her job.

3. **Auditing:** Regularly reviewing and assessing internal controls, processes, and systems to identify and address any issues or weaknesses both by the internal auditors and external auditors.

4. **Risk Management:** Identifying, assessing, and managing potential risks that could impact the organization's objectives.

INTERNAL CONTROL FRAMEWORKS (COSO, CADBURY)

COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private sector organization that provides guidance on internal control, including enterprise risk management and financial reporting. The COSO framework is widely recognized as the leading framework for internal control and provides a systematic and disciplined approach to risk management.

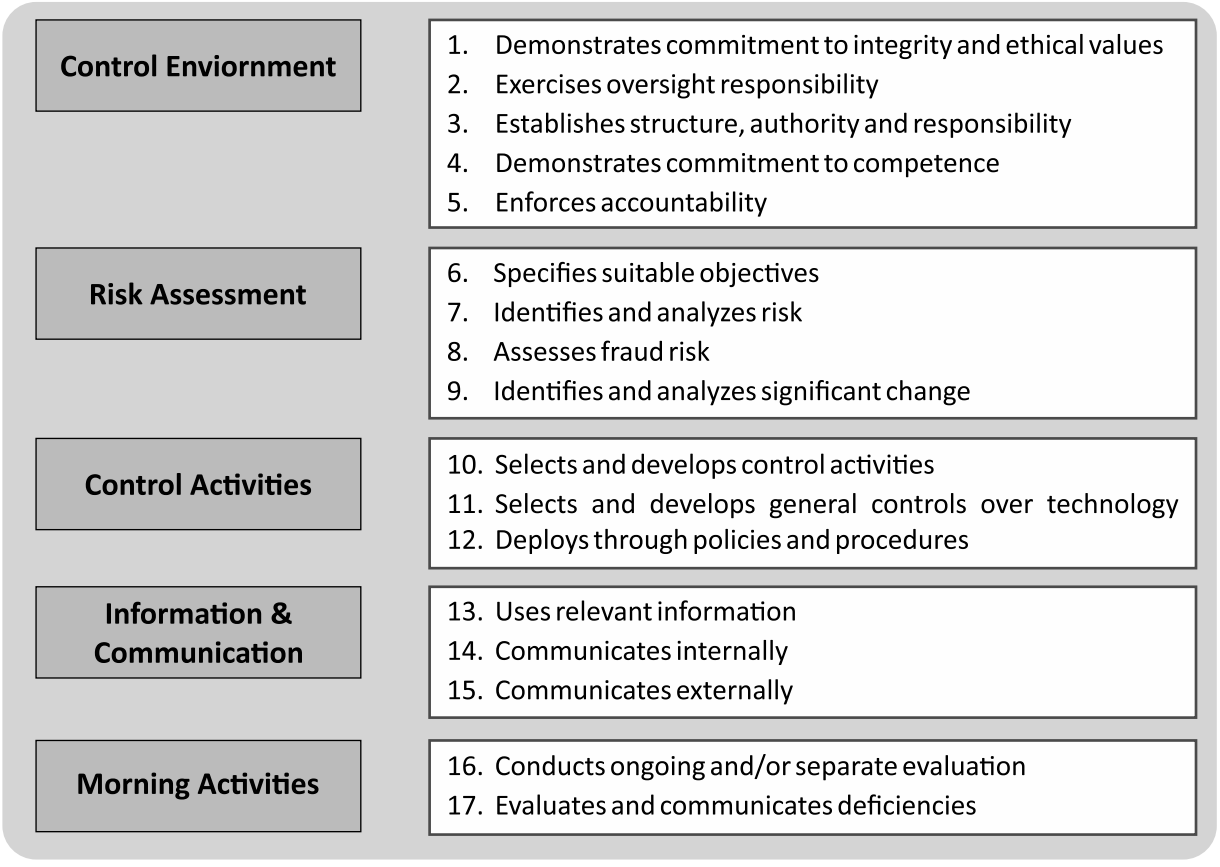
It provides a systematic approach for organizations to assess and improve their internal controls, with the goal of reducing the risk of fraud and other financial misstatements.

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control Framework is a widely recognized framework for assessing and improving the internal controls of an organization. It was first published in 1992, and the latest version was released in 2012.

The COSO Internal Control framework 2012 consists of five (5) interrelated components of internal control and seventeen (17) principles: Control environment, risk assessment, control activities, information and communication, and monitoring.

1. **Control environment** sets the tone for the organization and is the foundation for the other components. This component involves the tone at the top, the integrity and ethical values of the organization, and the way the organization manages risk.
2. **Risk assessment** component helps organizations identify, assess and prioritize the risks they face in achieving its objectives.
3. **Control activities** refer to the policies and procedures that are put in place to mitigate those risks.
4. **Information and communication** ensure that the necessary information is recorded, processed, and communicated effectively to support other components of internal control.
5. **Monitoring** refers to the ongoing assessment of the internal control system to ensure that it remains effective and relevant and communication of results to those charged with governance.

The updated COSO internal control framework 2012 provides guidance for organisations to assess and improve their internal control systems, with a focus on the achievement of objectives in the categories of operations, financial reporting, and compliance with laws and regulations. It is widely used by auditors, internal control professionals, and management to improve the effectiveness and efficiency of internal control systems.



Control Environment

1. The organisation demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. Identification and assessment of risks relating to objectives.
7. The organisation identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organisation identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organisation selects and develops general control activities over technology to support the achievement of objectives.
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into place.

Information and Communication

13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Cadbury Committee of United Kingdom

Sir George Adrian Hayhurst Cadbury was a British businessman and member of the Cadbury family. He is known for his role as chairman of the Cadbury Committee, which produced a report on corporate governance in 1992.

The Cadbury Committee, also known as the Financial Reporting Council (FRC), was established in 1991 in response to a series of corporate failures in the United Kingdom. It was formed in 1991 in the United Kingdom and was charged with reviewing the role and effectiveness of corporate governance in UK companies.

The Cadbury Report, which was published in 1992, established a set of principles for corporate governance and helped to raise the standards of corporate governance in the UK. The Cadbury Report was a landmark publication that set out principles for good corporate governance and helped to shape the modern understanding of corporate governance.

The Cadbury Report emphasized the importance of transparency, accountability, and independent oversight in corporate governance. It also introduced the idea of the board of directors being responsible for setting the tone at the top and setting the company's values and ethical standards.

The Cadbury Report had a significant impact on corporate governance practices in the UK and beyond, and its recommendations continue to be influential to this day. Both the COSO and Cadbury frameworks provide important guidance for organizations looking to improve their internal controls and governance practices. The COSO framework focuses specifically on internal control, while the Cadbury Report addresses broader issues of corporate governance. Both COSO and Cadbury are important references for internal control and corporate governance.

The COSO framework provides a comprehensive approach to internal control and risk management, while the Cadbury Report provides principles for effective corporate governance. Both frameworks continue to be widely used and are considered best practices for organisations looking to improve their internal control and governance processes.

SOX and Internal Controls over financial reporting (United States of America)

The Sarbanes-Oxley Act (SOX) was enacted in 2002 in United States of America in response to a number of high-profile accounting scandals, such as Enron and WorldCom that caused a loss of investor confidence in the reliability of financial reporting. The fundamental objective of this law was to protect the interest of investors by imposing new rules on accounting and financial transparency.

SOX was designed to restore public trust in the financial reporting of publicly traded companies by improving the accuracy and reliability of financial statements, strengthening internal controls, increasing transparency, and enhancing corporate governance.

The SOX seeks to prevent fraudulent financial reporting and corporate accounting irregularities by imposing stricter regulations and penalties on companies and their executives.

The Sarbanes-Oxley Act (SOX) requires companies to establish and maintain internal controls over financial reporting to ensure the accuracy and reliability of their financial statements. These controls are designed to prevent fraudulent financial reporting, provide reasonable assurance that financial information is complete and accurate, and safeguard company assets.

SOX mandates that the management of a company assess the effectiveness of its internal controls and provide an annual report to external auditors. Additionally, external auditors are required to review and attest to the effectiveness of a company's internal controls.

Steps for Establishing Internal Control

- Identify the key areas where the internal control system is to be established.
- Work flow should be designed in such a way that it is not complete if another person has not checked it. (Maker/ Checker concept)
- Establishing of surprise check mechanism where money plays a significant role. Example cash verification, inventory and other high value documents like title deeds.
- Review of units and facilities which are in remote locations.
- Reporting mechanism for non-adherence of key compliance areas.
- Vigil mechanism for larger entities as applicable.

ROLE OF INTERNAL AUDITORS IN IMPLEMENTATION OF INTERNAL CONTROLS

Internal auditors play a critical role in the implementation of internal controls. They provide assurance that internal controls are designed and operating effectively, and help identify areas where improvements can be made. Some key responsibilities of internal auditors in the implementation of internal controls are:

Assessing risk: Internal auditors assess the risks facing an organisation and make recommendations for controls that can mitigate these risks.

Evaluating existing controls: Internal auditors evaluate existing controls to determine their effectiveness and make recommendations for improvement.

Recommending controls: Internal auditors recommend new controls to address areas where risks are high and existing controls are not adequate.

Monitoring implementation: Internal auditors monitor the implementation of new and existing internal controls to ensure that they are operating effectively. They also perform regular follow-up audits to ensure that the recommended improvements have been made and that the control system remains effective.

Reporting: Internal auditors provide regular reports to management on the status of internal controls. Internal auditors communicate their findings to management and other stakeholders, including the board of directors. They provide recommendations for improving the control system and make suggestions for enhancing overall risk management. They identify any weaknesses or deficiencies in the control system and make recommendations for improvements.

Supporting compliance: Internal auditors support the organisation's efforts to comply with laws, regulations, and standards by evaluating the effectiveness of compliance controls.

Evaluating control design: Internal auditors evaluate the design of the internal control system to ensure it is effective and efficient. They review the documentation of the control procedures to determine if they are adequate to meet the company's objectives.

Testing control effectiveness: Internal auditors test the effectiveness of the internal control system by conducting audits and other evaluations.

The internal auditor should be familiar with STANDARD ON INTERNAL AUDIT (SIA) 11 "Consideration of Fraud in an Internal Audit" issued by the Institute of Chartered Accountants of India while conducting Internal Audit of any entity.

Providing training: Internal auditors provide training to employees on the importance of internal controls and how they can be used to support the organisation's goals and objectives.

EXAMINE THE EFFECTIVENESS AND EFFICIENCY OF INTERNAL CONTROLS

Internal controls are measures put in place by organizations to ensure the reliability of financial reporting, promote efficiency and effectiveness in operations, and compliance with laws and regulations. The effectiveness and efficiency of internal controls can be evaluated by examining several key aspects:

1. **Design:** The design of internal controls must be appropriate to address specific risks and must be able to effectively mitigate those risks. The controls should be designed in a way that does not create unnecessary complexity, which could lead to inefficiencies in the operations of the organisation.
2. **Implementation:** The internal controls must be properly implemented and be an integral part of the organisation's operations. This means that employees must be trained on the controls and be familiar with the procedures they need to follow.
3. **Monitoring:** The internal controls must be regularly monitored to ensure they are functioning as intended. This includes regular audits and reviews of the control environment to identify any weaknesses and make improvements as needed.
4. **Documentation:** Proper documentation of internal controls is essential to ensure that they are consistently followed and that any changes to the controls are properly recorded.
5. **Evaluation:** Periodical evaluation of the effectiveness and efficiency of internal controls is critical to ensuring they remain relevant and effective in mitigating risks. This includes ongoing monitoring and assessment, as well as periodic internal audits or external reviews. By regularly evaluating and improving the controls, organizations can ensure that they are able to operate effectively and efficiently, while minimizing risks to the organization and its stakeholders.

FRAUD RISK AWARENESS

Fraud risk awareness refers to the understanding and recognition of potential fraudulent activities that could harm an individual or an organization as well as the measures that can be taken to prevent or mitigate them. It encompasses being able to identify red flags and warning signs, understanding how fraudsters operate and taking proactive steps to mitigate potential losses.

Fraud can occur in various forms, including financial fraud, cyber fraud, identity theft, and more. By being aware of fraud risks is crucial in order to prevent or detect such activities and minimise the damage caused by fraud.

There are several steps that individuals and organizations can take to increase fraud risk awareness:

1. **Stay informed:** It is important for individuals and organizations to regularly assess and update their fraud risk awareness efforts to stay ahead of evolving threats. This can be done by staying informed about the latest fraud schemes, tactics and trends used by fraudsters, and implementing best practices for fraud prevention.
2. **Be vigilant:** Be cautious of any unusual or suspicious behavior and report it promptly.
3. **Protect personal information**: Keeping sensitive information such as social security numbers, bank accounts, and passwords secure and private.
4. **Implement security measures:** Using strong passwords, enable two-factor authentication, and install antivirus software on devices. Keep passwords secure and unique, and change them regularly.
5. **Train employees:** Educate employees on the latest fraud trends and how to recognize and prevent fraud.
6. **Monitor accounts regularly:** Regularly review bank and credit card statements and monitor accounts for any unusual or suspicious activity.

    - By being aware of the potential risks and taking proactive measures, individuals and organizations can reduce their vulnerability to fraud.

- Be cautious of unsolicited emails and phone calls, especially those that ask for personal information.
- Using strong anti-virus and anti-malware software to protect computer systems.
- Avoiding using public Wi-Fi networks for sensitive transactions, such as online banking.
- Be wary of too-good-to-be-true offers or deals that are not from a trusted source.

Fraud risk awareness is a critical aspect of protecting oneself and one's assets. By staying informed and taking proactive measures, individuals and organizations can reduce the risk of falling victim to fraudulent activities.

Understanding and documenting the system

Any entity be it a small entity, a large enterprise, a multinational company, Government, Bank, Insurance Company, Not for Profit organisations like Trust, Charitable Institutions need an adequate accounting system. This will enable them to control the business, safeguard the assets, prepare accounts and comply with legislation of the land. Hence, it is fundamental in order to carry out an effective internal audit or statutory audit, the auditor should gain an understanding of the existing accounting system and of the procedures and controls incorporated therein, sufficient for the purpose of his audit.

It is considered preferable that the processes necessary to understand and document the entity's accounting system and to evaluate the entity's system of internal controls to be conducted separately. It is then easier for the internal auditor to keep clearly in mind the differences involved in these two phases.

The documenting of the understanding of an entity's accounting system may be achieved as below:

1. An extended form of internal control questionnaire
2. Notes on accounting procedures or other narrative description
3. Flow charts.

For small business, certain of the procedures may not be appropriate. When reliance is not to be placed on internal controls, the auditor may only need brief notes of the clients' accounting system. A small business with few staff operating from one location might not warrant the preparation and completion of internal control questionnaires or flow charts.

Where the accounting system is complex, it is preferable for the internal auditor to use flowcharting techniques in conjunction, if necessary, with narrative descriptions to record his understanding of the system since flowcharting enables the auditor to obtain a better understanding of the system and to identify more easily the relevant control features in the system.

After having completed the flowcharts or notes on accounting procedures to document his understanding of the entity's accounting system, the auditor should confirm the understanding by carrying out a transaction review by way of walk-through test.

Transaction reviews: The transaction reviews should be documented, showing the operations reviewed and identifying the specific transaction selected. The results of the transaction review may conveniently be filled with the related flowcharts or notes on accounting procedures.

Narrative Description: The internal auditor prepares a written description of the system in use.

Internal Control Questionnaire: The internal auditor considering the size and nature of its business and based on the discussions with the management designs a set of questions, which when answered will document a number of aspects of the internal control system. This questionnaire is popularly known as internal control questionnaire (ICQ) and can be very useful in documenting and assisting the evaluation of controls.

Visual description: The internal auditor uses charts to make the system more visual and easier to understand. Organisational Chart, Audit trail flow chart (cradle to grave),Document flow chart and Systems flow chart used in documenting computer systems as application controls.

CASE STUDY

Pink collar crime – Largest municipal fraud in the history of United States

Rita Crundwell was a controller and treasurer of Dixon, Illinois from 1983 to 2012, operator of the largest municipal fraud in U.S. history. In 2011, one of the city commissioners praised her "she looks after every tax dollar as if it were her own".

Crundwell began working in city hall in 1970 when she was a high school student. She became Dixon's comptroller and treasurer in 1983 and opened the curious RSCDA account in December 1990.

In the fall of 2011, Crundwell took 12 weeks of unpaid leave. Kathe Swanson, the city clerk, had to fill in for Crundwell and prepare the fiscal report for an upcoming council meeting.

Crundwell had never enabled the online option for the city's bank accounts, so Swanson couldn't view and print the statements. And the city's bank, Fifth Third Bank, hadn't mailed the statements.

Crundwell would advise Swanson to give only the last four digits of the pertinent accounts to email to the bank so it could fax the records to city hall.

"Swanson finally called the bank, and said, 'I want every statement of the City of Dixon's faxed to me in the next five minutes,' "

When she got the bank records, she saw three large deposits — of $200,000, $300,000 and $500,000 into an unknown account called "RSCDA — Reserve Fund" or Reserve Sewer Capital Development Account.

"My first thought was that Rita put a private account under the city's name because she was buying and selling horses and shielding the money from the IRS," Swanson says.

"That's when I really started looking at all the debits and credits, like gasoline and things like that. Well, the city has their own pumps, so I knew it wasn't a city account." Swanson says Dixon funds would first go into the Illinois Treasurer's Investment Pool [ITIP] state account in Springfield, the capital, because of better interest rates.

"We would get a fax from the state saying the money was in the account, whether it was from state sales tax, income tax, whatever," she says. "Once the money was in the ITIP account, Rita would call it up before 11 o'clock, and it would go into our capital development account — an honest account.

Then before she left for lunch, she'd go over to the capital development account book, write a check for 'treasurer,' payable to treasurer.

She'd take that check and bring it over to Fifth Third Bank in Dixon and deposit it into the RSCDA account, 'care of Rita Crundwell, Treasurer, City of Dixon.' "

Crundwell did this 169 times until she'd stolen $53.7 million.

She was fired in April **2012** after the discovery that she embezzled **$53.7 million** from the city of Dixon for over **22 years** to support her championship American Quarter Horse breeding operation. She was sentenced to nearly **twenty years** in prison and is scheduled to release on October 2029. However, Rita Crundwell has been released from federal prison in central Illinois on August 18, 2021 and taken to an undisclosed location.

As an Internal auditor what are the learnings from this important case?

Solution:

Complete absence of internal control, internal check and lack of ethical behavior:

Rita Crundwell first opened the fictitious account in 1990, she was also the only signatory to operate the account. Many banks, including Fifth Third, require additional people or entities to be involved so as to prevent fraudulent activities. A resolution is also required to open up an account at the bank. This resolution never took place.

Rita would make "fictitious" checks simply addressed to "treasurer" rather than under her name or the city's name and deposit them into the fictitious account. This is not usual behavior, and according to a former manager at Fifth Third, checks should have been addressed to "treasurer of the City of Dixon" or "City of Dixon."

You have learned the term "segregation of duties." In this case, Rita ' s bookkeeping duties should have been separated — by having someone other than Rita approve expenses as well as reconciling bank statements.

Crundwell also wrote lots of checks for large sums of money, which, acted as a clear red flag. It appears that the bank had proper procedures in place in theory but did not enforce them.

Aftermath of Fraud done by Rita

The city of Dixon, Illinois has dramatically changed many of its practices to ensure nobody has the extent of power Rita had to commit fraud for so long.

After she was dismissed, the city hired a new finance director who reorganized the city's finances and restructured the department. She implemented more internal controls so that no one person could complete an entire process by him- or herself including her. Today the city has hired more clerks that specialize in specific areas such as payroll and billing. Mail is no longer picked up by one person. Instead, it is delivered straight to City Hall.

https://harbert.auburn.edu/binaries/documents/center-for-ethical-organizational-cultures/cases/dixon-fraud.pdf

RISK MANAGEMENT

Meaning of Risk

Risk is a possibility that something bad will happen. Contract risk management minimises the probable loss through the effective and efficient management. It evaluates risks in terms of probability of occurrence and its impact. A simple example is given below.

Modern problem of using phone while driving: The impact of using phone while driving can range from none, to a near-miss, to collisions of various intensity which can result in injury or death to the driver, their companions, other road users and innocent bystanders, and damage to property.

Types of Risks

Systematic Risk: The overall impact of the market due to COVID, inflation, corruption, change in interest rate etc.

Unsystematic Risk: Asset-specific or company-specific uncertainty due to employee turnover, strike, higher cost of operations etc.

Political/Regulatory Risk: The impact of political decisions and changes in regulation.

Financial Risk: The capital structure of a company (degree of financial leverage or debt burden).

Country Risk: Uncertainties that are specific to a country.

Operational Risk: Uncertainty about a company's operations, including its supply chain and the delivery of its products or services.

Environmental Risk: Uncertainty about environmental liabilities or the impact of changes in the environment.

Management Risk: The impact that the decisions of a management team have on a company.

Legal Risk: Uncertainty related to lawsuits or the freedom to operate.

Competition: The degree of competition in an industry and the impact choices of competitors will have on a company.

Obsolescence Risk: In the rapid changing world, risk of obsolescence is high. Kodak Camera, Nokia, Tape-recorder are real life examples. Netflix renting of DVDs.

Definition of Enterprise risk management (ERM) as per COSO

Enterprise risk management (ERM) is *"the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to opportunities to gain competitive advantage".*

The fundamental elements of ERM are the assessment of significant risks and the implementation of suitable risk responses.

Risk responses include:

- **acceptance or tolerance of a risk;**
- **avoidance or termination of a risk;**
- **risk transfer or sharing** via insurance, a joint venture or other arrangement; and
- **reduction or mitigation of risk** via internal control procedures or other risk prevention activities.

Due to increased globalization of the economy, Covid 19 has created a havoc across the continents. Complete involvement on the part of board members and employees is essential in determining the risk appetite of a company, and in identifying and prioritising risks. Speed of onset and persistence of risks, in addition to impact and likelihood, are important considerations in the prioritisation of risks.

Continuous monitoring and concise reporting on key risk exposures are essential for effective risk management. Other important ERM concepts include: the risk philosophy or risk strategy, risk culture and risk appetite. These are expressions of the attitude to risk in the organisation, and of the amount of risk that the organisation is willing to take. These are important elements of governance responsibility.

A Risk Management Plan

A defined and documented process agreed upon by stakeholders for how risks will be identified, assessed, a decision made on mitigation (or if the risks will be accepted), how a response plan will be developed and what controls will be put in place to monitor risks.

Identify Risks: A way to efficiently capture identified various risks and add to the risk register.

Risk Register: A log of identified risks and their status. Risks are added to the register as they are identified and the impact and probability of occurrence are assessed through qualitative and quantitative methods.

Qualitative / Quantitative Analysis Tools: Methods for analysing / evaluating the probability and impact of risks on the organisation's objectives.

Response / Mitigation Plan: Determine if the risks are acceptable or not based on assessment and plan for mitigation.

Control Risks: Assess effectiveness through methods like risk audits and continually improve the project execution.

Risk Mitigation: The objective of risk mitigation is to reduce the probability and/or consequences of a risk event to an acceptable threshold and define appropriate response.

Questions To Ask:

- What are the available options?
- Tradeoffs (cost / benefit) of each option?
- Impacts of current decisions on options?

Risk mitigation actions may be costly and time consuming; Actions taken are balanced against priority level of the risk. Organisations typically transfer risk where possible, for example through product warranty or taking an insurance cover. Low-risk factors may be recognised by the Organisation but absorbed as a matter of policy.

Management responsibilities include:

- the risk architecture or infrastructure,
- documentation of procedures or,
- risk management protocols,
- training, monitoring and reporting on risks, and
- risk management activities.

Every entity exists to realise value for its stakeholders. Value is created, preserved, or eroded based on the management decisions in all activities right from setting strategy to operating the enterprise on day-to-day basis.

COSO Enterprise Risk Management (ERM)– Integrated Framework

The COSO Board released in September 2017 an update to the 2004 Enterprise Risk Management–Integrated Framework

ENTERPRISE RISK MANAGEMENT

The ERM Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity. Tone at the top is a popular buzzword.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organisation can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organisation.

Five Components Twenty Principles

Governance and Culture	Strategy and Objective-Setting	Performance	Review and Revision	Information, Communication, and Reporting
1. Exercise Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyses Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communications Risk Information 20. Reports on Risk, Culture, and Performance

RECOMMEND CONTROLS TO PREVENT AND DETECT FRAUD AND EDUCATE TO IMPROVE THE ORGANIZATION'S FRAUD AWARENESS

There are several controls that an organization can implement to prevent and detect fraud, and education is a crucial component in improving an organization's fraud awareness.Here are some recommendations for controls and educating across the entity:

1. **Segregation of duties:** Ensure that no single person has control over multiple aspects of a process or transaction. For example, the person who approves a purchase should not be the same person who pays for it. Maker, Checker and Approver is an excellent tool to prevent errors and frauds.
2. **Rotation of duties**: Ensure that there is periodical rotation of duties for key positions. We saw in the largest municipal fraud that in the absence of rotation of duties, huge fraud perpetrated by one employee gone unnoticed. Punjab National Bank fraud also happened due to absence of mandatory job rotation or transfer of few employees of the branch.
3. **Mandatory vacation:** Having a HR policy for giving mandatory vacation to key employees helps the employees to come fresh after vacation and also prevents employees from hiding their tracks of crime.
4. **Treat employees well**. It has been observed that if the employees are treated well by giving timely rewards and recognition for their work, they feel motivated. If they are treated badly like being underpaid or overlooked for promotion, they look for the opportunity and rationalise to do frauds to take revenge on their employers.
5. **Regular audits**: Conduct regular internal audits especially at remote locations where there are significant projects being executed or manufacturing facilities are run to identify potential fraud and ensure compliance with internal controls.
6. **Background checks**: Conduct thorough background checks on employees, especially those in positions of trust or responsibility.
7. **Whistleblower hotline:** Implement a confidential hotline for employees to report suspicious activity without fear of retaliation.
8. **Use of technology:** Implement fraud detection software and use data analytics to identify patterns of suspicious activity.
9. **Fraud awareness training:** Provide periodical training to all employees on the types of fraud that can occur, how to identify it, and how to report it. Also ensure that adequate documents are kept in HR as evidence to prove that the employee participated in the training and understood it. This will help on a later date if the fraudulent employee feigns ignorance.
10. **Code of conduct:** Establish a code of conduct that clearly defines ethical behavior and expectations for employees.
11. **Management oversight and Tone at the top:** Ensure that management regularly reviews and approves transactions and financial statements. Ensure that independent directors are really independent.
12. **Reinforce accountability:** Hold employees accountable for their actions and ensure that consequences are enforced when necessary.
13. **Document retention:** Establish policies for the retention and destruction of records to ensure that important documents are not lost or destroyed.

Communicate all key changes to Policies and Procedures of the entity to all stakeholders like employees, vendors, customers and document evidence in support of the same that these stakeholders have read and understood the implications of changes made.

By implementing the above controls and providing education on fraud prevention and detection, organizations can help protect themselves against potential fraud and improve their overall fraud awareness.

ROLE OF INTERNAL CONTROL IN THE NEW DIGITAL ERA

Robotic Process Automation (RPA)

Companies across industries are working to digitize parts of the business with robotic process automation (RPA), often referred to as "bots." RPA involves the use of software robots to automate routine, repetitive, and rules-based tasks that were previously performed by humans. By automating these tasks, RPA can reduce errors, increase efficiency, and improve the accuracy and timeliness of data.

RPA bots are programmed to perform tasks in a consistent manner, which reduces the risk of errors and inconsistencies in data. By automating processes, RPA can also reduce the risk of human error.

RPA can provide an audit trail of all activities performed by the bots. This means that auditors can easily track and verify activities, which can improve the accuracy of financial statements and reduce the risk of fraud.

Enhanced monitoring and reporting: RPA can provide real-time monitoring and reporting of activities, which can help identify and address potential issues quickly. This can be particularly valuable in areas such as compliance, where organizations need to demonstrate adherence to regulations and policies.

Reduced operational risks: RPA can help reduce operational risks by automating tasks that are susceptible to errors or require significant manual effort. This can lead to more efficient processes and lower operational costs.

However, it's important to note that while RPA can enhance internal controls, it's not a substitute for a strong internal control system. Organisations still need to establish and maintain effective internal controls that are aligned with their business objectives and risks. Additionally, RPA implementation should be carefully planned and monitored to ensure that it is working effectively and in compliance with relevant regulations and policies.

Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are revolutionising various industries, including the field of internal control. Internal control refers to the processes, procedures, and systems that an organization has in place to ensure that it operates efficiently, effectively, and ethically.

AI and ML can enhance internal control by automating repetitive and time-consuming tasks, providing insights into patterns and anomalies, and reducing the risk of fraud and errors. Here are a few examples of how AI and ML can improve internal control:

Fraud detection: AI and ML algorithms can analyse large amounts of data to detect patterns that may indicate fraud. These algorithms can also learn from historical data to identify new patterns and adapt to changing fraud tactics.

Risk assessment: AI and ML can be used to identify and assess potential risks, such as cybersecurity threats or compliance violations. By analysing data from various sources, these technologies can provide a more comprehensive and accurate risk assessment.

Process automation: AI and ML can automate routine processes, such as data entry or invoice processing, reducing the risk of human error and freeing up time for internal control professionals to focus on higher-value tasks.

Predictive analytics: By analysing historical data and identifying outliers, AI and ML can predict future trends and patterns, helping organizations make informed decisions about internal control measures and resource allocation.

However, it is important to note that AI and ML are not a replacement for human expertise and judgment. These technologies should be used in conjunction with internal control professionals to ensure that the insights they provide are accurate and relevant.

Additionally, organisations must be mindful of ethical considerations, such as bias and privacy, when implementing AI and ML in their internal control processes.

Blockchain Technology

Blockchain is a digital ledger technology that is used to store data in a secure and decentralised way. It offers numerous benefits for internal control in various industries. One of the key benefits of blockchain for internal control is its ability to provide an immutable record of transactions. This means that once data is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network participants. This feature ensures that the data is trustworthy and tamper-proof, which is critical for maintaining a strong internal control environment.

Another benefit of blockchain for internal control is its ability to provide transparency and accountability. Since all transactions are recorded on a shared ledger, all network participants have access to the same information. This makes it easier to identify discrepancies, detect errors, and investigate fraud.

Furthermore, blockchain can automate various internal control processes, such as transaction approvals, reconciliation, and audit trails. Smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code, can be used to automate these processes, ensuring accuracy and consistency.

In summary, blockchain can improve internal control in a number of ways, including providing a secure and tamper-proof record of transactions, enhancing transparency and accountability, and automating internal control processes. As a result, blockchain is increasingly being adopted by businesses across various industries to strengthen their internal control environment.

Cloud Computing

Cloud computing is a technology that allows users to access computing resources, such as servers, storage, applications, and services, over the internet. Internal control, on the other hand, is a process designed to provide reasonable assurance regarding the achievement of an organization's objectives in terms of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

When it comes to cloud computing, internal control is essential to ensure that the organization's data, systems, and processes are secure and reliable. Here are some ways internal control can be implemented in the context of cloud computing:

Risk assessment: The organisation should conduct a risk assessment to identify potential risks associated with using cloud computing services, such as data breaches, system failures, and vendor lock-in.

Vendor selection: The organisation should select cloud computing vendors that meet its security and compliance requirements. This may include evaluating vendors' security controls, certifications, and audit reports.

Service level agreements (SLAs): The organisation should negotiate SLAs with cloud computing vendors that define the level of service, performance, and availability that is required. The SLAs should also include provisions for data privacy, security, and compliance.

Access controls: The organisation should implement access controls to ensure that only authorized personnel can access its cloud computing resources. This may include using multi-factor authentication (MFA), role-based access control, and encryption.

Data encryption: The organisation should encrypt data before storing it in the cloud, to prevent unauthorized access and data breaches.

Monitoring and reporting: The organisation should implement monitoring and reporting mechanisms to detect and report security incidents and data breaches. This may include using intrusion detection systems, log monitoring, and vulnerability scanning.

Overall, internal control is critical to the effective and secure use of cloud computing services, and should be an integral part of an organisation's cloud computing strategy.

PRACTICE QUESTIONS

1. **While planning an audit, the auditor does not think that it would be necessary to understand internal controls. Advise the auditor in this regard.**

   Solution: The auditor shall obtain an understanding of internal control relevant to the audit. Although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment whether a control, individually or in combination with others, is relevant to the audit.

2. **The team member of the auditor was of the view that understanding the internal control of the company would not help them in any manner in relation to audit procedures to be applied while conducting the audit.**

   Solution: The view of the team member of the auditor is incorrect because understanding the internal control of the company would help the auditor and his team members in designing the nature, timing and extent of audit procedures to be applied while conducting the audit of the company.

3. **One of the team members of the auditors was of the view that risks that were identified during the course of audit were not required to be documented. Explain with a reason whether the viewpoint is justified.**

   Solution: The auditor shall document the identified and assessed risks of material misstatement at the financial statement level and at the assertion level; and the risks identified, and related controls about which the auditor has obtained an understanding. Keeping in view the above, the viewpoint is not justified because risks that were identified during the course of audit were required to be documented by the auditors.

4. **One of the directors of the Company was of the view that internal financial controls have nothing to do with accounting records of a company. Comment.**

   Solution: The meaning of internal financial controls as, "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information." In view of above, viewpoint of director is incorrect.

5. **The office manager controlled the company's financial operations. She did payroll, accounts payable, invoicing and cash receipts. She rarely took time off, and even then, came back when they needed to run checks or payroll. The owner viewed her as key to running the business. What are your recommendations as an internal auditor of the organizations in view of evaluating Internal Control?**

   Solution:

   - Segregation of duties is critical so that everything isn't done by one person. Having one person do everything can lead to fraud and theft. Oversight can help, but segregation of duties is the best alternative.
   - Take the three primary cash responsibilities such as accounts payable, accounts receivable, and payroll. Cross train others so that they can take over if needed.
   - Provide close oversight of cash operations.

CASE STUDY

1. Credit Suisse Crisis

Background

The second largest 167-year-old Swiss bank, Credit Suisse was bailed out by UBS (Union Bank of Switzerland- one of the predecessor firms' name), the biggest number one Swiss Bank by doing a buy out and the AT1 bonds of Credit Suisse Bank worth 17 BN $ were completely written off.

A bailout is when an individual, business, or organization provides capital or other resources to a failing company to prevent it from collapsing.

UBS agreed to buy rival bank Credit Suisse for 3 billion Swiss francs ($3.23 billion) and assume up to $5.4 billion in losses, in a shotgun merger planned by Swiss authorities. Under the deal, on the orders of the Swiss regulator, 16 billion Swiss francs ($17 billion) of Credit Suisse's Additional Tier 1 debt will be written down to zero.

Credit Suisse had made a few questionable acquisitions and had been penalized many times, the reputation of the bank was in question leading to a tremendous slowdown in all its businesses, and on 3-year average business growth for most of its segment was negative over 10% YoY.

Due to negative sentiment about Credit Suisse bank, by December 2022 just in a couple of months, huge deposits of over 150 billion were withdrawn from the bank.

The problem faced by Credit Suisse bank was different as compared to Silicon Valley Bank (SVB) which had an ALM mismatch. In the case of Credit Suisse, there were changes in the top management many times. This had put a lot of liquidity pressure on the bank & news of the SVB crisis led to another panic situation triggering further liquidity crisis for the Bank.

The collapse of Credit Suisse could impact Switzerland's reputation as a stable, strong country for banking.

Reasons for downfall of Credit Suisse

In 2021, the collapse of the U.S. family investment fund Archegos Capital and British finance firm Greensill Capital triggered a pre-tax loss of close to $1 billion for Credit Suisse Bank.

Following the collapse of Archegos, Credit Suisse's investment bank CEO and chief risk and compliance officer left the company. An independent investigation of Credit Suisse's role in the Archegos scandal found that the bank had failed to "effectively manage risk," but suggested that no fraudulent or illegal conduct occurred.

Chairman Antonio Horta-Osorio resigned in January 2022 from the company as he broke COVID-19 quarantine regulations. Rumor is circulated that Credit Suisse Bank faces impending failure, prompting clients to pull about $119 billion in funds in the last quarter of the year. Credit Suisse in March 2023 said it will borrow up to $54 billion from the Swiss National Bank. U.S. institutions Silicon Valley Bank and Signature Bank failed, setting the global financial system on edge.

Material Weaknesses in Financial controls over financial reporting and risk assessments

In its Annual Report 2022 Credit Suisse Bank management admitted "material weaknesses" in its internal controls over financial reporting and risk assessments in 2022 and 2021. "As of December 31, 2022, the Group's internal control over financial reporting was not effective, and for the same reasons, management has reassessed and has reached the same conclusion regarding December 31, 2021."

Credit Suisse's 'material weaknesses' mainly related to the failure to design and maintain effective risk assessments; and this problem has been vastly seen in its financial statements.

Credit Suisse also failed to design and maintain effective monitoring activities relating to management oversight, resource allocation, and deficiency assessment. This lack of oversight and monitoring made it difficult for the bank to identify and address issues before they become major problems.

Controls over consolidated statements of cash flows were inadequate

Finally, Credit Suisse's material weakness disclosure revealed that their controls over the classification and presentation of the consolidated statement of cash flows were inadequate. This resulted in revisions to their previously issued financial statements,

Auditor PricewaterhouseCoopers (PwC) in their report included an "adverse opinion" on the effectiveness of the bank's internal controls over its reporting, but its financial statements "present fairly, in all material respects" the financial position of the bank in 2020 through 2022.

2. Silicon Valley Bank Collapse

Background

Silicon Valley Bank (SVB) was founded in the year 1983 at Silicon Valley, California. It was the 16th largest U.S. bank before its collapse. SVB specialized in financing and banking for venture capital-backed startup companies -- mostly technology companies. Venture capital firms did business there as well as several tech executives. SVB had assets totaling $209 billion at the end of 2022, according to the Federal Deposit Insurance Corporation (FDIC).

The Silicon Valley Bank (SVB) failure is the largest bank failure since 2008.It's been a long time since the last failure that was as big as this one, which was Washington Mutual.

Reasons for collapse of Silicon Valley Bank

Many of SVB's customers were tech startups and hence a concentration of money from just one sector. Due to rising inflation rates and other things, many companies started struggling to get additional financing from venture capital and elsewhere. So, they needed to withdraw their deposits at SVB. When one industry suddenly needed cash, many companies went to the bank and tried to withdraw all their money. That's a run on the bank.

A bank doesn't have all that cash on hand. SVB, had invested that money. When these tech startups wanted all their money in cash it resulted in a run on the bank. SVB had invested it in low-yield treasury bonds that would pay interest. But given the rate of inflation — the interest rate was under 2%, very low — the bonds were worth more if they were held for a long time.

But the Bank had to sell them quickly and at a loss. So, what happened was it incurred a huge loss. As a result, Bank management tried to raise more money by issuing their own bonds on the open market.

Lack of diversification

Silicon Valley Bank invested a large amount of bank deposits in long-term U.S. treasuries and agency mortgage-backed securities. However, bonds and treasury values fall when interest rates increase.

When the Federal Reserve hiked interest rates in 2022 to combat inflation, SVB's bond portfolio started to drop. SVB would have recovered its capital if they held those bonds until their maturity date.

SVB used to lend out money in short durations. However, in 2021, they shifted to long-term securities such as treasuries for more yield, and they did not protect their liabilities with short-term investments for quick liquidations. They were insolvent for months because they could not liquidate their assets without a large loss.

SVB didn't have the cash on hand to liquidate the deposits as they were tied up in long-term investments. They started selling their bonds at a significant loss, which caused distress to customers and investors.

Within 48 hours after disclosing the sale of assets, the bank collapsed.

California Department of Financial Protection & Innovation appointed the Federal Deposit Insurance Corporation (FDIC) as receiver. California regulators shut the bank down on March 10, 2023.

Unlike personal banking, SVB's clients had much larger accounts. It didn't take long for money to diminish during the bank run, with the escalating pace of withdrawals causing a snowball effect. Most customers had deposits more than the $250,000 FDIC limit.

SVB stockholders and investors took a big hit because, unlike customers, they were not backed by FDIC on their investment. Large tech companies with significant cash in SVB include Etsy, Roblox, Rocket Labs and Roku.

SVB purchased by First Citizens Bank

On March 26, 2023, FDIC announced First Citizens Bank will purchase Silicon Valley Bank and assume the majority of its deposits and loans. As of March 10, Silicon Valley Bank reported nearly $167 billion in total assets and $199 billion in deposits.

First Citizens Bank will purchase about $72 billion in assets at a discounted rate of $16.5 billion. FDIC will remain in control of nearly $90 billion in assets and securities in its receivership. All 17 of Silicon Valley Bank's branches will operate under Silicon Valley Bank, a division of First Citizens Bank.

The FDIC also estimated that the SVB failure cost nearly $20 billion.

Mismatch of ALM – Major reason

One of the key issues with SVB was the ALM (asset-liability management) mismatch, where they invested short-term funds into long-term securities.

The bank had made an ill-informed and reckless bet that the Fed would keep interest rates low and thus, when the Fed hiked aggressively SVB's unrealized bond losses soared. Interest rates and bonds have an inverse relationship which means as interest rates rose, bond prices fell, resulting in the massive loss-making bond portfolio.

One of the major rating's agencies, Moody's, subsequently downgraded SVB' credit rating. In response to downgrading, SVB announced its intention to raise $2.25 billion in fresh capital by selling new shares, which didn't go down well with the market. The sheer size of SVB's illiquid 'held-to-maturity' investments (poorly performing bond portfolio) spooked depositors who realized it would be near impossible to liquidate the sizeable holdings into cash to meet withdrawals in the event of a run on the bank.

SVB had inadequate risk management and internal controls that struggled to keep pace with its growth,

SVB's failure brought with it the demise of Signature Bank – a favourite banking institution for the crypto industry – and Silvergate Bank.

LESSON ROUND-UP

- As per Section 134 of the Companies Act, 2013, the term "Internal Financial Controls" means the policies and procedures adopted by the company for ensuring, orderly and efficient conduct of business, including adherence to company's policies, safeguarding of its assets, prevention and detection of frauds and errors, accuracy and completeness of the accounting records, and timely preparation of reliable financial information.
- Objectives and various Dimension of Internal Control.
- Difference between Internal check and Internal Control.
- Types of Control – Preventive, Detective, Input , Output.
- Benefits and Limitation of Internal Control.
- Internal Control Techniques such as Segregation of duties, Access Control, Auditing, Risk Management.
- Internal Control Frameworks (COSO, CADBURY).
- Implementation of internal controls: Internal auditors play a critical role in the implementation of internal controls. They provide assurance that internal controls are designed and operating effectively, and help identify areas where improvements can be made.
- Role of Internal Control in the New Digital Era such as:
  - (i) Robotic Process Automation (RPA)
  - (ii) Artificial Intelligence
  - (iii) Block chain Technology
  - (iv) Cloud Computing.

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

MCQs Based Questions

1. Internal check is meant for:
   - (a) Prevention of frauds
   - (b) Detection of frauds
   - (c) Helping audit in depth
   - (d) Detection of errors.

   Answer: (c) Helping audit in depth.
2. Internal controls and internal check are:
   - (a) One and the same
   - (b) Different
   - (c) Internal control includes internal check
   - (d) None of the above.

   Answer: (c) Internal control includes internal check

3. In comparison to the independent auditor an internal auditor is more likely to be concerned with –
   (a) Cost accountancy system
   (b) Internal control system
   (c) Legal compliance
   (d) Accounting system.

   Answer: (b) Internal control system.

4. Which of the following is responsible for establishing a private company's internal control?
   (a) Management
   (b) Auditors
   (c) Management and auditors
   (d) Committee of Sponsoring Organizations.

   Answer: (a) Management.

5. Internal controls can never be considered as absolutely effective because:
   (a) their effectiveness is limited by the competency and dependability of employees
   (b) not all organizations have internal audit departments
   (c) controls are designed to prevent and detect only material misstatements
   (d) Internal controls prevent separation of duties.

   Answer: (a) their effectiveness is limited by the competency and dependability of employees.

6. An act of two or more employees to steal assets or misstate records is frequently referred to as:
   (a) collusion
   (b) material weakness
   (c) control deficiency
   (d) Significant deficiency.

   Answer: (a) Collusion.

7. The process of ensuring no single employee is in control of receiving, recording, and authorizing a transaction is known as _____.
   (a) authorization
   (b) segregation of duties
   (c) accuracy
   (d) completeness.

   Answer: (b) segregation of duties.

8. Due to inherent limitations of internal control system it can provide _____ assurance that its objectives are achieved.
   (a) Reasonable

(b) Absolute

(c) Negative

(d) All of these.

Answer: (a) Reasonable.

9. A Graphic presentation of internal controls in the organisation and is normally drawn up to show the controls in each section or subsection is known as:

(a) Narrative Records

(b) Check List

(c) Internal Control Questionnaire

(d) Flowchart.

Answer: (d) Flowchart.

10. Internal check is a check on _____ transactions whereby work carried out by one person is checked by _____.

(a) Unusual; auditor

(b) Unusual; another

(c) Day-to-day; auditor

(d) Day-to-day; another.

Answer: (d) Day-to-day; another.

11. When more persuasive audit evidence is needed regarding the effectiveness of a control:

(a) It may be appropriate to increase the extent of testing of the control and reduce the extent of the degree of reliance on controls

(b) It may be appropriate to decrease the extent of testing of the control as well as the degree of reliance on controls

(c) It may be appropriate to decrease the extent of testing of the control and increase the extent of the degree of reliance on controls

(d) It may be appropriate to increase the extent of testing of the control as well as the degree of reliance on controls.

Answer: (d) It may be appropriate to increase the extent of testing of the control as well as the degree of reliance on controls.

12. The objective of internal audit is:

(a) To prevent errors and frauds

(b) To detect errors and frauds

(c) To improve financial controls

(d) All of the above.

Answer: (d) All of the above.

Practical Questions:

1. "The auditor shall obtain an understanding of the major activities that the entity uses to monitor internal control over financial reporting" Explain.
2. Obtaining an understanding of the entity and its environment, including the entity's internal control, is a continuous, dynamic process of gathering, updating and analysing information throughout the audit. Analyse and explain giving examples.
3. What are the limitations of Internal Control?
4. What are the benefits of Internal Control?
5. Explain the role of Internal Auditor in implementing the effective Internal Control System.
6. What are the various types of control that are required in every organisation?
7. What do you mean by COSO Internal Control Framework? Explain its various components and Principles.
8. Explain what do you mean by the term Enterprise Risk Management? What are the various components and principles prescribed in COSO Enterprise Risk Management Integrated Framework?
9. Internal control role in this digital era of RPA, Blockchain, Artificial Intelligence and Machine learning and Cloud computing.

Case Study

Sam and his brother Bob owners and operators of tractors for 30 years as a closely held business. A local bank was financing them based on the inventory of tractors worth millions of Rupees. Their wives were sharing the accounting duties.

Both wives of the brothers retired from business because of their age. James son of Sam who was a graduate was appointed as the accountant. Earlier, James would approve vendor invoices, Julie will prepare cheques which will be signed by either of brothers.

The brothers entrusted with Sam all aspects of bookkeeping, accounts payable, accounts receivable, payroll and accounts reconciliations. Later on they also gave him cheques signing authority and credit card in the name of the company.

James got married and his personal expenses increased and he soon found it difficult to maintain the life style he had known when he was a bachelor and living with his parents.

Having been under financial pressure, he looked for the opportunities to make extra money from the company. He used the company funds and started manipulating the books of account to hide his crime for maintaining his life style. The brothers initially had attributed the cash flow problem to a downturn in the economy. But later on wanted to know why there is a regular cash crunch in the business even after economy was slowly improving.

One of James cousin, Daniel a CA with more than 5 years of experience was appointed to do an internal audit on behalf of the owners discovered the fraud, when he was going through the bank statements. Several cheques were issued by James to himself on a regular basis. When confronted, James confessed to the crime of embezzling thousands of rupees.

You are required to submit a detailed internal audit report on various aspects of the case based on the concepts given in this study lesson and give appropriate recommendations to the owners.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's

- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Internal Audit Engagements and Planning

Lesson 4

KEY CONCEPTS

■ Audit Planning ■ Audit Universe ■ Audit Programme

Learning Objectives

To understand:

- What is Audit Plan?
- How to develop the Audit Plan?
- What are the steps involved in Audit Planning?
- Benefits for formulating Audit Plan
- How to obtain knowledge of the client's business?
- What is Audit Universe?
- Factors for developing Internal audit universe.
- How to supervise Audit Engagement?
- How to monitor Audit Engagement Outcomes?

Lesson Outline

INTRODUCTION

World has witnessed many industrial revolutions that has transformed the way business are owned, conducted and governed. The first industrial revolution was referred as proto-industrialization period that started at the end of the 18th century to the beginning of the 19th century. This was followed by second industrial revolution at the end of the 19th century, with massive technological advancements in new source of energy. Last few decades of 20th century witnessed the Third Industrial Revolution, where we saw emergence of nuclear energy, rise of electronics, telecommunications and, of course, computers. With these transformation changes business operations have become complex day by day with high volume of transactions carried out at multiple locations with increasing dependency on technology. Further to carry out such large and complex operations organizations are compelled to delegate and decentralize tasks and authorities.

Thereby, stakeholders including Board of Directors, senior management, shareholders, lenders, investors and government are concerned with the controls, transparency and probity of the transactions carried out on daily basis and there arises need to have strong governance, transparent operations and reporting of underlying gaps, errors or frauds for initiating appropriate actions on proactive basis. Accordingly, the stakeholders get internal audit conducted to obtain report on the deficiency in internal controls system and underlying transactions for better governance of organization and take timely remedial actions wherever needed.

Traditionally internal auditing was being performed as one time activity with dual verification on documentation and vouchers. There has been a steep rise in the trend of frauds over the last couple of decades and regulators have also become more vigilant towards the requirement of strong internal control system which resulted in the announcement of statutory obligations viz. Sarbanes Oxley Act in USA, Listing and Disclosure Requirements of SEBI and Company's Act, 2013 & rules there-under. Additionally Internal Audit have become mandatory for certain class of companies as per Company's Act.

Internal auditor is expected to review business processes and various transactions to provide report to management on adequacy of internal controls. With the large volume transactions and complexity of the business processes, it is not possible for Internal Auditor to check 100% of the business transactions. Therefore, internal auditor is normally expected to focus on areas of high risk and he needs to adopt sampling techniques for verification of transactions and form his opinion. This leaves him with inherent risk of some material misstatement or gaps remains undetected. Also, there are many challenges being faced by the internal auditors in performance of their duties. The major challenges include:

- Mismatch in the expectations from and output of the internal audit function
- Audit Risk
- Uncertainties due changing environment – internal as well as external.

Audit Risk - Audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR).

AUDIT PLANNING

Planning an audit involves:

(a) Establishing the overall audit strategy

(b) Developing an audit plan

"The auditor should plan his work to enable him to conduct an effective audit in an efficient and timely manner. Plans should be based on knowledge of the client's business".

a) acquiring knowledge of the client's accounting systems, policies and internal control procedures;

b) establishing the expected degree of reliance to be placed on internal control;

c) determining and programming the nature, timing, and extent of the audit procedures to be performed; and

d) coordinating the work to be performed.

An effective planning performed with the scientific approach to identify the critical aspects and transaction to be coveted in audit, is the only mechanism to manage these challenges effectively and reduce audit risk.

In the case of Companies under Companies Act, 2013, it is a legal requirement for the Audit Committee or its Board of Directors to formulate the overall internal audit plan of the company. Companies (Accounts) Rule 13(2) of Companies Act, 2013 provides: "The Audit Committee of the company or the Board shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity, and methodology for conducting the internal audit."

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the Institute of Chartered Accountants of India (ICAI), The Audit Committee or the Board takes the active support of the Chief Internal Auditor, to develop the Overall Internal Audit Plan, in consultation with the Executive Management.

Further, as per the standards of Internal Auditing, 2010 – Planning issued by "International Standards for The Professional Practice of Internal Auditing", "The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals."

A well-structured Risk Based Internal Audit planning allows internal audit to provide reasonable assurance to the Board of Directors and other stakeholders that most critical activities have been audited by the auditor and whether or not underlying controls are designed and working effectively to mitigate major risks of the Company.

Benefits of Audit Planning

a) Helping the auditor to devote appropriate attention to important areas of the audit.

b) Helping the auditor identify and resolve potential problems on a timely basis.

c) Helping the auditor properly organize and manage the audit engagement so that it is performed in an effective and efficient manner.

d) Assisting in the selection of engagement team members with appropriate levels of capabilities and competence to respond to anticipated risks, and the proper assignment of work to them.

INTERNAL AUDIT LIFE CYCLE

A Typical internal audit engagement comprises of following five phases.

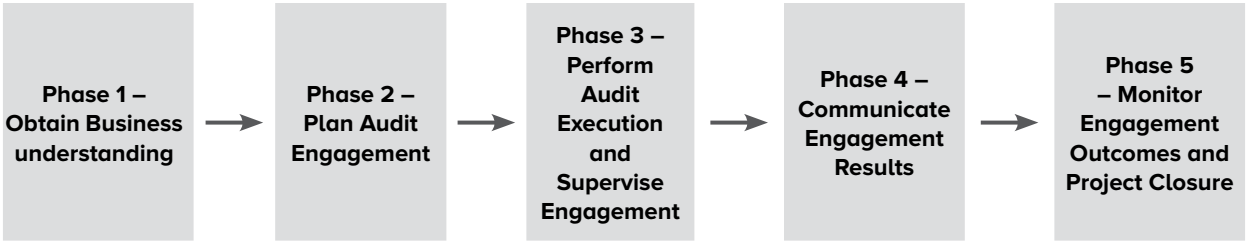
Phase 1 – Obtain Business understanding

Phase 2 – Plan Audit Engagement

Phase 3 – Perform Audit Execution and Supervise Engagement

Phase 4 – Communicate Engagement Results

Phase 5 – Monitor Engagement Outcomes and Project Closure



All of these steps are required to be performed while performing any Internal Audit engagement in the same sequence. Let us see some of the major activities to be performed under each of these steps.

PHASE 1 – OBTAIN KNOWLEDGE OF THE CLIENT'S BUSINESS AND ITS ENVIRONMENT

Effective planning is the key to success for every project. As discussed earlier, it is essential for every Internal Auditor to prepare an effective audit scope and plan to focus on most essential activities and transactions, which is not possible without obtaining a good understanding of the business strategy, its operations, its organization structure, locations and offices, product and business segments, financial overview of the business, applications statutory compliances and various other internal and external factors impacting the organization.

Internal Auditor must plan and conduct meetings with various stakeholders including Board of Directors, Senior management person, Head of Departments and other business associates and partners to obtain understanding of the organization's business environment, organization's vision, mission and top management's expectations from the audit functions.

Following steps may be followed for obtaining the knowledge of the Business and its environment. The internal auditor should obtain a level of knowledge of the entity sufficient to enable him to identify events, transactions, policies and practices that may have a significant effect on the financial information. Following are some of the sources wherefrom the internal auditor can obtain such knowledge:

- Organization's policy and procedures manual.
- Its ownership and governance structures.
- The way that the entity is structured and how it is financed.
- Annual financial statements and annual report.
- Minutes of the meetings of the shareholders, board of directors, and important committees of the board such as the audit committee, remuneration committee, shareholders' grievances committee.
- Legislation and regulations that significantly affect the entity.
- Management reports/ internal audit reports of prior periods.
- Newspaper/ industry journals.
- Discussion with client's management and staff.
- Visits to entity's plant facilities etc. to obtain firsthand information regarding the production processes of the entity.
- Visits to the entity's department where the accounting and other documents are generated, maintained, and the administrative procedures followed..

Internal auditor must also obtain understanding of the underlying Information Technology landscape, various applications and ERP systems of the organization and Management Information System of the organization.

PHASE 2 – PLAN AUDIT ENGAGEMENTS

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the ICAI, Internal audit planning is conducted at two levels:

a) An overall internal audit plan for the entire entity is prepared for a given period of time (usually a year) and presented to the highest governing body responsible for internal audits, normally, the Board of Directors, or the Audit Committee.

b) A number of specific internal audit plans are prepared for individual assignments to be undertaken covering some part of the entity and presented to the Chief Internal Auditor.

Once auditor has obtained the business understanding and managements expectation from the internal audit, next step would be to plan the audit engagements in two stages:

A. Prepare Risk Based Internal Audit Universe and Audit Plan.

B. Prepare Audit Work Plan based on overall Internal Audit Plan.

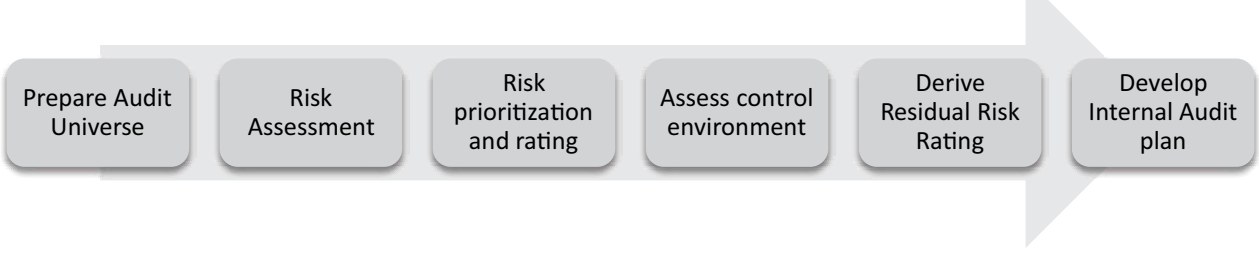
A. Prepare Risk Based Internal Audit Universe and Audit Plan

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the ICAI, Internal audit plan for the entire entity is prepared for a given period of time (usually a year) and presented to the highest governing body responsible for internal audits, normally, the Board of Directors, or the Audit Committee. Also, the internal auditor shall undertake an independent risk assessment of all the Auditable Units identified in the Audit Universe and align this with the risk assessment conducted by the management and the statutory auditor. This is required to priorities and focus audit work on high-risk areas, with due attention to matters of importance, complexity and sensitivity. The internal auditor may also plan to undertake a dedicated audit of the company's Risk Management Framework and processes, as a separate review or assignment.

Accordingly, internal audit planning should be based on organizational risk assessment wherein the internal auditor identifies the significant risks of the process and the underlying control environment established by the organization to mitigate such risk or bring it down to an acceptable level. Based on the risk assessment and control environment assessment of all the processes that may be audited, Internal Auditor can assess the frequency and level of effort and focus that need to be dedicated for performing detailed audit of the process.

E.g., High Risk areas may be audited more frequently (every quarter / year) and less risky areas may be audited at lesser frequency. Such a process is termed as Risk Based Internal Audit Planning. Such Internal Audit scope and plan must be approved by Audit Committee or Board of Directors. Once approved, Internal Auditor must share detailed Audit Plan with the key managerial personals and plan in advance the detailed schedule of the Internal Audit to be conducted.

Risk Based Internal Audit Planning can be performed in following phases:



1. Prepare Audit Universe

Audit universe in simple terms defined as everything. It includes all of space, and all the matter and energy that space contains. Hence, universe may be referred to set of all the components and elements that may be referred. Accordingly, in terms of Internal Audit engagements, Audit Universe would refer to all the process, activities, departments, locations, functions that may be subject to audit by the Internal Audit team, also referred to as auditable entity.

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the Institute of Chartered Accountants of India, Audit Universe and Scope of Coverage: Prior to defining the scope of internal audit, a complete identification of all the Auditable Units (locations, functions, business units, legal entities, including third parties where relevant) of the organization shall be made. This list of all the Auditable Units is, generally, referred to as the "Audit Universe".

On the basis of business understanding obtained, Internal Auditor must list down all the auditable entities for the organization. E.g., Purchase process, Sales Process, Human Resource process, Particular plant location or branch office, Finance process, Research and Development department etc.

Auditor must keep in mind some important factors in mind while developing the internal audit universe:

- Organization vision, mission and objectives
- Expectations from the internal audit function
- Organization structure and setup – E.g., Centralized / Decentralized
- Geographic location of the Organization
- Scalability of the operations
- Organic linkage between the business process/ sub processes
- Sufficiency to justify cost and effort involved for auditing the underlying auditable entity

Extract of Audit Universe of a typical Manufacturing Company

Sr. No.	***Department***	***Business Locations***			
		Corporate Office	***Plant***	***Regional Office***	***Branch Office***
1	Procurement	✓	✓		
2	Sales Process			✓	✓
3	Marketing & Promotions	✓		✓	
4	Vendor Bill Payments	✓	✓		
5	Collections	✓		✓	✓
6	Payroll	✓	✓		
7	Human Resources	✓	✓		
8	Financial and Account	✓	✓		
9	Information Technology	✓	✓		
10	Statutory Compliances	✓	✓	✓	✓

Illustration 1:

Mr. ABC is the chief Internal Auditor of M/s XYZ Pharmaceuticals Private Limited. The company has spread its sales operations across 20 countries through Distributors and Dealers network. For the purpose of local connections and compliances, the Company has opened branch offices in each country. Apart from this, the Company has manufacturing facilities in India and China. For the purpose of manufacturing raw material, technology is imported from various countries including USA, France and Japan. The key statistics of the company are mentioned below:

1. Annual Turnover of the Company – Rs. 25,000 crores approx.
2. Total Manpower – 8000 employees
3. Total Branches – 18

Audit Committee has asked Chief Internal Auditor (CIA) to prepare audit plan for 3 years. Please suggest the steps to be followed by the CIA and prepare audit universe of the Company.

Response:

Chief Internal Auditor needs to follow the structured step by step approach for identifying all auditable entities as part of audit universe. Following steps need to be followed for preparing the comprehensive audit universe and audit plan for the Company:

- Prepare Audit Universe to identify all auditable entities of the Company.
- Risk Assessment to identify key risks and materiality to audit a particular area as a separate and standalone area with dedicated focus.
- Risk prioritization and rating to assess significance and criticality of identified auditable area.
- Assess control environment to assess the controls in place.
- Derive Residual Risk Rating to assess the criticality of the audit area after factoring the controls in place and identify the areas that need immediate attention.
- Develop Internal Audit plan after considering the resources in hand and criticality of the audit area. This is needed to do justice with any area being audited and pick up more critical area first and at more frequently.

Considering the nature of the Company and after assessing the criticality and locations of various operations of the company, following audit universe may be prepared by CIA.

Sr. No.	***Department***	***Business Locations***		
		Corporate Office	**Plant Locations**	**Branch Offices (20)**
1	Sales Operations	✓		
2	Schemes and Incentives	✓		✓
3	Dealer and Distributor Management			✓
4	Procurement and Supply Chain		✓	

5	Contract Management		✓	
6	Material Management		✓	
7	Loan Licensing Manufacturing		✓	
8	Plant Operations		✓	
9	Plant Maintenance		✓	
10	Quality Assurance and Quality Control		✓	
11	Information Technology	✓	✓	✓
12	Research and Development	✓	✓	
13	Human Resource	✓	✓	✓
14	Payroll Function	✓	✓	✓
15	Country Operations / Branch Office Review			✓
16	Intangible Assets	✓		
17	CRO - Clinical Research Operations	✓		

Following points are pertinent to note in the highlighted audit universe:

1. Audit areas which are critical either due to large expenditure and quantum of operations or due to critical business risks may be audited separately e.g., schemes and incentive and Loan License Manufacturing in the above illustration.
2. Areas which need to be physically visited by the team to review may be audited as a separate area. E.g., Branch office and overseas operations in above example.
3. Each plant and each branch office may also be defined as auditable entity depending on quantum of operations at particular plant or branch office.

2. Risk Assessment

Once the audit universe is formalized and finalized in discussion with management, next step is to identify all major Risks applicable to the respective auditable entities identified under risk universe. This includes evaluation of 'what can go wrong' in the particular process/ function which can have any adverse impact on the organization. Risk and adverse impact on the organization need to be studied under measurable tangible losses or intangible impacts in the form of reputation of inefficiencies. It is vital to assess the all major/key risk in the process being studies for comprehensiveness and completeness of the risk identification exercise.

3. Risk Prioritization and rating

The identified risks need to the prioritized based on the pre-defined criteria typically on the scale of 1 to 5 as mentioned below:

- Score 1 - Insignificant
- Score 2 – Low
- Score 3 – Moderate
- Score 4 – Major
- Score 5 – High

Auditor need to assess the risks and provide ratings to the risk basis professional judgement after considering the following factors:

1. Direct / indirect risks associated
2. Risk of statutory non compliance
3. Quantified Financial Loss
4. Threat to Health, Safety & Environment
5. Reputation risk
6. Possibility / History of frauds or major irregularity
7. Complexity (Volume of business, nature of business)
8. Results of earlier audits external/ Internal
9. ESG (Environmental, Social, Governance) impacts of actions.

4. Assess control environment

The main objective of risk assessment and prioritization is to assess the criticality of the process / auditable entity at inherent level. However, internal auditor should arrive at the residual risk after factoring the controls established by the organization to mitigate such risks. Internal Auditor must assess the controls environment and provide control environment rating to each of the auditable entity.

The International Standards for the Professional Practice of Internal Auditing (Standards) Glossary defines the control environment as "The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides discipline and structure for the achievement of the primary objectives of the system of internal control.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the updated Internal Control - Integrated Framework in 2013. The framework states "The control environment is the standards, processes and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. The control environment comprises the integrity and ethical values of the origination; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control."

Following factors need to be kept in mind while performing the assessment of control environment:

1. Preventive or detective controls in place
2. Strong monitoring of Legal compliance
3. IT enabled controls and IT security initiatives
4. Corporate governance structure
5. Documented Policy and Procedures
6. Organization's sensitivity towards Health, Safety & Environment
7. Fraud detection mechanism
8. Governance over decentralized operations.

Overall control environment can be rated typically on the scale of 1 to 5 as mentioned below:

- Score 1 – Very Strong
- Score 2 – Strong
- Score 3 – Moderate
- Score 4 – Weak
- Score 5 – Almost missing

5. Derive Residual Risk Ratings

There are two elements of a risk:

- Preliminary Risk Assessment Rating.
- Control Environment Rating.

Both these ratings can be multiplied together to give a single measure of the significance of a risk, or a residual risk. For example, high risk of procurement being carried out at higher prices, the control environment rating could be weak or strong depending on system enabled approval process or comparison of quotation hence residual risk could be high or low.

Residual Risk Rating Score = Preliminary Risk Assessment x Control Environment Rating

The overall process and auditable entity could be classified as High, Medium or Low depending on residual risk rating of the process: Following criteria may be used:

1. High – For Residual rating >= 15
2. Medium – For Residual rating between 8 and 15
3. Low – For Residual Rating =< 8

Extract of Risk Assessment, Control Environment Assessment and Residual Risk rating of a sample procurement process

Sr. No.	*Auditable Entity*	*Sub Process*	*Initial Risk Rating*	*Rationale for initial risk rating*	*Control environment rating*	*Rationale for control environment rating*	*Residual Risk Rating*
1	Procurement	Planning and Budgeting	4	Vendor favoritism and High risk of financial loss due to purchase at high prices	1	Strong IT system enabled approval process. Techno commercial assessment and approval by independent committee.	4
		Requisition and Selection					
		Contracting and Ordering					
		Receiving					
		Quality check and Invoicing					
		Payment processing					

Illustration 2:

Mr. ABC is the chief Internal Auditor of M/s XYZ Pharmaceuticals Private Limited. The company has spread its sales operations across 20 countries through Distributors and Dealers network. For the purpose of local connections and compliances, the Company has opened branch offices in each country. Apart from this the Company has manufacturing facilities in India and China. For the purpose of manufacturing raw material, technology is imported from various countries including USA, France and Japan. The key statistics of the company are mentioned below:

1. Annual Turnover of the Company – Rs. 25,000 crores approx.
2. Total Manpower – 8000 employees
3. Total Branches – 18

The company has received notice from the regulatory authorities for some non-compliance noted in adhering to the quality standards and one of the competitive companies has also filed a suit on the company for using their patented formulae. Company has increased its sales by 20% in current year and profitability by 35%.

Company has well documented Delegation of Authority, policies and procedures and SAP is implemented to records of transactions and provides MIS on timely basis.

Audit Committee has asked Chief Internal Auditor (CIA) to prepare audit plan for 3 years. Please suggest the key risks to be considered by the CIA against each auditable entity of the audit universe and assess the control environment. Prepare the heat map with the areas falling under High / Medium / Low risk categories.

Response:

Given the company has managed to increase sales with higher increase in profitability, the internal control environment of the Company appears to be comfortable. Further the company has well defined policies and Delegation of Authority and SAP is also implemented in the organization which provides reasonable comfort on good governance and control environment at the Company. Although the same needs to be tested during the audit.

With this information the Chief Internal Auditor may prepare the following summary of risk assessment, control environment assessment to finally arrive at the residual risk ratings so that critical and other areas can be categorized under High, Medium and Low.

Sr. No.	***Department***	***Risk Assessment***	***Risk Rating***	***Control Assessment***	***Control Rating***	***Residual Risk Rating***	***Residual Risk Rating***
1	Sales Operations	Annual sales of company being INR 25,000 Cr. and being sales push organization, it has high risk of incorrect sales reporting.	5	Policies and procedures are documented. SAP is implemented for recording transactions. Finance team monitors sales on weekly basis.	2	10	Medium

Sr. No.	*Department*	*Risk Assessment*	*Risk Rating*	*Control Assessment*	*Control Rating*	*Residual Risk Rating*	*Residual Risk Rating*
2	Schemes and Incentives	Considering high value of schemes and incentives paid by the Company, this is high risk to be audited separately.	5	Policies and procedures are documented. SAP is implemented for recording transactions. Finance team calculates and reviews on monthly basis.	2	10	Medium
3	Dealer and Distributor Management	Company operated largely on the Distributor and Dealer model who invest in company's stock and support in managing working capital.	3	Dealer onboarding procedure is well documented. Compliance is ensured by finance team.	2	6	Low
4	Procurement and Supply Chain	Company works on a long-term contract with dedicated supplier and imports from other countries. Terms are agreed and adhered.	4	Policies and procedures are documented. SAP is implemented for recording transactions. Finance team independent approval is required for all transactions.	1	4	Low
5	Contract Management	Company works on a long-term contract with dedicated supplier and imports from other countries. Terms are agreed and adhered.	3	Policies and procedures are documented. Process of legal vetting is implemented before signing all contracts.	2	6	Low

Sr. No.	Department	Risk Assessment	Risk Rating	Control Assessment	Control Rating	Residual Risk Rating	Residual Risk Rating
6	Material Management	Material is critical aspect of operations. There are some high risks for quality of material handling and storage norms to followed.	5	Policies and procedures are documented. Regular training is provided to workers for ensuring compliance to policies.	4	20	High
7	Loan Licensing Manufacturing	A LLM agreement is entered by the company that authorize company to market and manufacture the drugs. Ensuring compliance to the terms is critical and high risk for the Company.	5	Policies and procedures are documented. Independent finance checks are implemented for compliance.	4	20	High
8	Plant Operations	Plant is completely automated to follow fixed standards.	3	Policies and procedures are documented. SAP is implemented for recording transactions. Plant head is experienced and regular monitoring of operations is being done.	3	9	Medium

Sr. No.	*Department*	*Risk Assessment*	*Risk Rating*	*Control Assessment*	*Control Rating*	*Residual Risk Rating*	*Residual Risk Rating*
9	Plant Maintenance	Plant needs to be maintained on regular basis and the operations are done as per fixed schedule of dedicated team.	3	Policies and procedures are documented. SAP is implemented for recording transactions. Plant head is experienced and regular monitoring of maintenance is being done.	3	9	Medium
10	Quality Assurance and Quality Control	Being critical nature of operations and compliance norms to be followed by the company for ensuring good quality, this is high risk area.	5	Policies and procedures are documented. SAP is implemented for recording transactions. Quality checks are ensured as per compliance requirement and ISO standards.	3	15	High
11	Information Technology	Information technology system is outsourced to external company however considering the criticality of confidential information being handled, it is important to regularly monitor the controls on this area.	4	Operations are outsourced and SLAs are monitored on monthly basis.	4	16	High

Sr. No.	*Department*	*Risk Assessment*	*Risk Rating*	*Control Assessment*	*Control Rating*	*Residual Risk Rating*	*Residual Risk Rating*
12	Research and Development	There are high R&D expenditures incurred by the company.	4	Policies and procedures are documented. SAP is implemented for recording transactions. R&D expenses are closely monitored by management and finance performs independent review.	3	12	Medium
13	Human Resource	Considering low rate of attrition in the company and high satisfaction index. Further, no major surprise noted in last 5 years.	3	HR policies and procedures are documents. Regular TAT and KPIs are monitored by management.	2	6	Low
14	Payroll Function	No major surprise noted in last 5 years. Rate of attrition is low and payroll is processed by outside vendor to ensure all compliance and confidentiality.	3	HR policies and procedures are documents. Regular TAT and KPIs are monitored by management.	2	6	Low
15	Country Operations / Branch Office Review	Branch offices deals with local distributors and support in co-ordination activities only.	3	Policies and procedures are documented. SAP is implemented for recording transactions.	2	6	Low

Sr. No.	*Department*	*Risk Assessment*	*Risk Rating*	*Control Assessment*	*Control Rating*	*Residual Risk Rating*	*Residual Risk Rating*
16	Intangible Assets	Company has large intangible assets of various patents and copy rights.	4	Policies and procedures are documented. SAP is implemented for recording transactions. Finance monitors all recording and valuation of intangible assets.	2	8	Low
17	CRO - Clinical Research Operations	Company has entered into contract with reputed hospitals and the same is working effectively for last 5 years.	3	Norms are documented and compliance to all requirements is ensured by a dedicated team reporting to COO directly.	2	6	Low

6. Develop Internal Audit plan

Depending on management requirement, 3 to 5 year internal audit plan can be developed considering the nature of business, business environment, objective of the management and expectations from the internal audit. Further, with certain calibration of the complete assessment being done annually, and based on inputs from Board of Director and audit committee, low- risk areas could be audited every three years, moderate-risk areas could be audited every other year, and high-risk areas audited every year. The audit plan should be revisited each year for new or changed risk factors.

Extract of Audit Plan of a typical Manufacturing Company

S. No	*Auditable Entity*	*Residual Risk Rating*	*Audit Frequency*	*Audit Plan*
1	Procurement	High	Every Year	Y1 , Y2, Y3
2	Sales Process	Low	Once in 3 years	Y1
3	Marketing & Promotions	Medium	Once in 2 years	Y1, Y3
4	Vendor Bill Payments	Medium	Once in 2 years	Y2

5	Collections	High	Every Year	Y1 , Y2, Y3
6	Payroll	Low	Once in 3 years	Y2
7	Human Resources	Medium	Once in 2 years	Y1, Y3
8	Financial and Account	Low	Once in 3 years	Y3
9	Information Technology	Medium	Once in 2 years	Y2
10	Statutory Compliances	Medium	Once in 2 years	Y1, Y3

Illustration 3:

Mr. ABC is the chief Internal Auditor of M/s XYZ Pharmaceuticals Private Limited. The company has spread its sales operations across 20 countries through Distributors and Dealers network. For the purpose of local connections and compliances, the Company has opened branch offices in each country. Apart from this the Company has manufacturing facilities in India and China. For the purpose of manufacturing raw material and technology is imported from various countries including USA, France and Japan. The key statistics of the company are mentioned below:

1. Annual Turnover of the Company – Rs. 25,000 crores approx.
2. Total Manpower – 8000 employees
3. Total Branches – 18

The company has received notice from the regulatory authorities for some non-compliances noted in adhering to the quality standards and one of the competitive companies has also filed a suit on the company for using their patented formulae. Company has increased its sales by 20% in current year and profitability by 35%.

Company has well documented Delegation of Authority, policies and procedures and SAP is implemented to records of transactions and provide MIS on timely basis.

Audit Committee has asked Chief Internal Auditor (CIA) to prepare audit plan for 3 years. CIA has prepared the audit universe, identified key risks against each auditable entity of the audit universe and assessed the control environment.

Please suggest the appropriate audit plan on behalf of CIA to be submitted to the audit committee for approval.

Response:

Basis these factors and other risk assessment carried out by the Chief Internal Auditor; the following audit plan may be proposed to audit committee for approval. The CIA also need to ensure that the risk assessment and audit plan is reviewed every year and required adjustment is done and re-submitted to audit committee for approval. This is critical to ensure that all recent changes and immediate priorities of the Company are factored in the audit plan and coverage.

Sr. No.	***Department***	***Residual Risk Rating***	***Audit Frequency***	***Audit Plan***		
				Y1	***Y2***	***Y3***
1	Sales Operations	Medium	Once in 2 years	✓		✓
2	Schemes and Incentives	Medium	Once in 2 years		✓	

Sr. No.	Department	Residual Risk Rating	Audit Frequency	Audit Plan		
				Y1	Y2	Y3
3	Dealer and Distributor Management	Low	Once in 3 years	✓		
4	Procurement and Supply Chain	Low	Once in 3 years		✓	
5	Contract Management	Low	Once in 3 years			✓
6	Material Management	High	Every year	✓	✓	✓
7	Loan Licensing Manufacturing	High	Every year	✓	✓	✓
8	Plant Operations	Medium	Once in 2 years	✓		✓
9	Plant Maintenance	Medium	Once in 2 years		✓	
10	Quality Assurance and Quality Control	High	Every year	✓	✓	✓
11	Information Technology	High	Every year	✓	✓	✓
12	Research and Development	Medium	Once in 2 years	✓		✓
13	Human Resource	Low	Once in 3 years		✓	
14	Payroll Function	Low	Once in 3 years	✓		
15	Country Operations / Branch Office Review	Low	Once in 3 years	All Branches to be reviewed in three years on cyclic basis.		
16	Intangible Assets	Low	Once in 3 years		✓	
17	CRO - Clinical Research Operations	Low	Once in 3 years			✓

B. Prepare Audit Work Plan based on overall Internal Audit Plan

Before starting any particular audit engagement, detailed work plan must be prepared by the audit managers and approved with Head of Internal Audit / Chief Internal Auditor. The work plan must be prepared after performing the evaluation of all major underlying risks in the process being reviewed and the audit checks to be performed to assess the adequacy of the control environment to mitigate such risks.

As per standard on Internal Audit (SIA) 220 - Conducting Overall Internal Audit Planning, issued by the ICAI, a number of specific internal audit plans are prepared for individual assignments to be undertaken covering some part of the entity and presented to the Chief Internal Auditor. Internal Auditor can plan the audit engagement as per the Standard on Internal Audit (SIA) 310 issued by The Institute of Chartered Accountants of India - Planning the Internal Audit Assignment.

The main objective for preparing the detailed audit plan for any process are:

1. Ensure all the requirement and management expectations from the audit are factored. Audit (Engagement) Plan and also in line with stakeholder.
2. Ensure that the scope and coverage of the process is comprehensive for providing reasonable assurance.

3. Allocate adequate time and resources to the engagement.
4. Ensure all identified and major risks are reviewed and tested during the audit and audit procedures are conducted in an efficient and effective manner.
5. Ensure the audit is performed in accordance to the applicable standards, regulatory requirements and available guidance.

A typical audit work plan would consist of following elements:

1. Mega and Sub process being reviewed
2. Key activities involved in underlying process
3. Underlying risk in the activities / sub-processes
4. Audit Checks to be performed
5. Sample criteria and sample to be used
6. Data required for audit.

Identification of underlying risk is the important activity for the purpose the purpose of preparing a comprehensive and qualitative audit plan. Internal Auditor should Identify and priorities risks based on detailed process documentation / process map and after considering following:

- Nature and type of errors and omissions that could occur, i.e., what could go wrong that would prevent the process from achieving its objectives
- For Financial / Reporting Risks - Evaluate whether the financial statement assertions are being met (Timeliness, Completeness, Accuracy, Authorization)
- Review risks / issues identified on other assignments for the same processes, risks common in industry
- Consider IT risks (access, backup, security, data integrity etc.)
- Be aware of common frauds/common methods of cooking books.

Extract of audit work plan of a Procurement Process

Activity	Key Risks	Control Description	Questionnaire	Samples	Detailed Testing
Procurement Planning & budgeting	Excess / short procurement due to inadequate procurement planning leading blockage of working capital / delay in production	Annual Purchase Plan for Current Items and Non-Current Items is prepared by Executive – Purchase based on annual sales plan, existing stock, buffer stock, etc. and the	• Whether the process of budgeting procurement is defined? • Inquire whether the budget is monitored at regular intervals? • Whether variance analysis is	Approved budget sheet Actual expenditure from ERP	• Completeness check on budget and actual details captured in ERP • Budget vs actual variance trend analysis. • Review the process of preparing purchase budget and its approval as per Delegation of Authority (DOA)

Activity	Key Risks	Control Description	Questionnaire	Samples	Detailed Testing
		same is reviewed and approved by designated authority as per DOA.	documented and reviewed along with reason analysis.		• Review the process of analyzing budget vs actual process and check whether approval for any variances were obtained. • For sample variances noted during above review perform root cause analysis and document reasons.

PHASE 3 – PERFORM AUDIT EXECUTION AND SUPERVISE ENGAGEMENT

Internal Auditor should perform audit engagement as per the documented audit work plan. However, audit plan should be modified and updated on the basis of additional knowledge and information gathered by the auditor during the course of audit to ensure audit activities are more effective and practical. Following steps should be planned and implemented performed while conducting the audit execution:

a. Prepare detailed audit schedule comprising of all key activities to be performed, meetings to be conducted, interviews to be conducted, data analytics to be done, on field verification and checks to be performed, identification and reporting of preliminary issues, conduct management discussion, obtain management agreed action plan, audit conclusion and reporting.

b. Internal Auditor must conduct the opening meeting with key stakeholders before start of audit engagement and share details of Information and System Access required to perform the audit.

c. Internal Auditor must obtain the required information and perform checks to ensure correctness and integrity of information received. To the extent possible, Internal Auditor must obtain the information directly from the source.

d. Perform data analytics to identify trends, outliers and initial exceptions.

e. Select sample and perform detailed audit checks for the sample information.

f. Detailed audit testing must be performed as per the audit work plan. Internal Auditor must ensure adequate evidences must be collected and stores in accordance to Standard on Internal Audit (SIA) 320, Internal Audit Evidence.

g. Identify gaps and initial exceptions.

h. Prepare issue sheets and identify root cause, implication and suggest remedial action plan and control to be implemented.

i. Adequate document of the internal audit work papers needs to be ensured as per Standard on Internal Audit (SIA) 330, Internal Audit Documentation.

Supervision of Audit Engagements

Continuous supervision of all audit activities should be performed by the person responsible for performing the audit and deputed by the audit committee and Board of Directors for the purpose of submitting internal audit report. Hence, audit supervision and control is required at all stages of audit including the following:

1. Audit Scoping
2. Audit Planning and Scheduling
3. Audit work plan and finalization of audit checks
4. Opening meeting with stakeholders
5. All key audit meetings
6. On-field review of audit checks being performed
7. Review of initial exceptions
8. Detailed review of draft report and final report
9. Concluding meetings with the management.

Internal Auditor must prepare detailed listed of the Identified audit issues and controls gaps. Interim reports may be issued after proper review of the work performed as per the Standard on Internal Audit (SIA) 350, Review and Supervision of Audit Assignments.

PHASE 4 - COMMUNICATE ENGAGEMENT RESULTS

Communicating audit engagement results effectively is the very crucial aspect of the audit engagement. Internal Auditor must prepare a draft issue, draft report of all the audit issues identified during the audit engagement and the same must be communicated to the relevant management personal and concluded with agreed action plan to be implemented for improving internal controls.

Every Internal Audit Report should include the following:

- Process and Audit Scope reviewed
- Locations Covered
- Audit timelines followed
- Information audited and source of information
- Sample selected and Criteria
- Rating Criteria used
- Audit period covered
- Executive Summary for senior management
- Distribution list
- Summary of all audit issues noted
- Audit Limitations, if any
- Implementation status of previous audit issues
- Notes to carry forward audit.

Detailed issue sheets should include the following:

- Title – What is the issue?
- Detailed Observation – Detailed explanation of the issue or gap?
- Risk Rating – Critical / Major / Moderate
- Root cause - Why did this happen?
- Exposure / Impact - So what? What is the risk? What is Implication of risk?
- Recommendation - What do we do now?
- Management comments with clear action plan
- Responsibility and Due date.

Following key considerations should made in communicating audit issues:

- Communication with client management should take place throughout the audit process
- Audit issues/reports should be communicated in detail with crystalize risk / exposure and specific business impact.
- In case of any fraud / Red Alert, issue must be reported on timely basis to the highest appropriate level of management keeping in mind confidentiality and sensitivity of the issues.
- Must ensure that all the audit issues noted during the audit are part of the draft and final audit report issued to the management.
- Proper review of the audit report is done by the Chief Audit Executive or Audit In-charge before communicating results with the management.

Internal Auditor should thereafter circulate Final Report and presentation his findings to the Audit Committee. Internal auditor must adhere to Standard on Internal Audit (SIA) 360, Communication with Management and Standard on Internal Audit (SIA) 370, Reporting Results while sharing the result of internal audit with the stakeholders.

Illustration 4:

Mr. ABC is the Chief Internal Auditor (CIA) of M/s XYZ Infrastructures Private Limited. The company has 4 projects ongoing being supervised by 4 different project in-charge. Mr. ABC had planned to audit each of the project once in a year sequentially. Accordingly, each project is being audited one in four years.

While performing the audit for one of the projects, the audit team come across some manipulation in the vendor invoices and noted that significant overpayment has been made to certain vendors.

Please suggest the immediate course of action to be taken by the audit team and CIA to handle the matter and key steps to be taken to report such issue to appropriate authority.

Response:

In the normal course of audit and reporting, the CIA is supposed to follow the communication and reporting protocols as mentioned in Internal Audit charted and reporting and communication guidelines of the standards on Internal Audit. In case of any exceptional scenario as highlighted in the above circumstances, the CIA must evaluate the situation in light of following factors:

1. Criticality of the issues that need to be highlighted i.e., the business risk or impact that it may bring to the organization.

2. Need for timely action to address the issue and protect value and reputation for the organization.
3. Level of confidence established to classify the identified gap as fraud or error.
4. Level of confidence and reasonable doubts on the people involved in such manipulations.
5. Evidences collected and recorded as working paper to establish the certainty of the issue noted.
6. Confidentiality to be maintained for any such significant issue to decide mode of communication and management level / audit committee members to be notified for such discrepancies.
7. Additional / subsequent audit procedure that still needs to be performed for concluding the issues and impact of early reporting on such procedures.

CIA must decide the appropriate course of action and reporting of such issues proactively in the interest of the company. Whilst generally timely communication should be made to top management / audit committee, if reasonably certainty of the will-full misconduct and/or major loss to the organization is established.

PHASE 5 - MONITOR ENGAGEMENT OUTCOMES AND PROJECT CLOSURE

Internal auditor must adhere to Standard on Internal Audit (SIA) 360, Communication with Management and Standard on Internal Audit (SIA) 390, Monitoring and Reporting of Prior Audit Issues. It must be ensured that audit engagement is effective and its benefit is realized by the organization which is possible by timely implementation of audit recommendation and its continuous heal check-up.

The main objectives of the monitoring include:

1. Adequate and timely monitoring of action taken against all open issues from prior audits.
2. Revalidation of the process and sample transaction to assess the effectiveness of the action taken.
3. Timely escalation to the senior management for initiating directions or alternate recourse to mitigate risk.

For the purpose of monitoring the engagement outcomes effective, a detailed action taken report of prior audit findings should be prepared by the internal auditor and reported to the Board of Director or Audit Committee along with the detailed internal audit report of the current period. The following steps must be followed for the purpose of preparing Action Taken Report:

1. Prepare summary of all open issues along with action plan and map responsible person notified for the action.
2. Identify all open issue overdue for action as per the agreed target implementation timelines.
3. Circulate all identified issues to the responsible persons for feedback and update on action taken by them.
4. For all the issues where action is not implemented or partially implemented – Obtain revised action plan and timelines for implementation along with reason of not implementing as per previous target dates.
5. For all issues where action plan is confirmed to be implemented – Perform sample validation of the process and transaction and assess the outcome to decide if the action plan is implemented or not. Revised action plan and timelines for issues found not implemented effectively during sample revalidation.
6. Prepare summary of the action taken with the details of issues not implemented to be reported to the Board of Director or Audit Committee.

Depending on the audit charter and direction from the audit committee, internal auditor may consider to re-assess the audit rating for all not implemented issues in light of the current business environment and open risk for the organization.

Illustration 5:

Mr. ABC is the Chief Internal Auditor (CIA) of M/s XYZ Infrastructures Private Limited. Mr. ABC has prepared a detailed Risk Based Internal Audit plan approved by the Audit Committee. During his audit of year 1, Mr. ABC noted 10 High risk rated issues and 25 medium and low risk rated issues. Audit Committee has directed the CIA to monitor the implementation plan for these audit issue and provide periodic report to the audit committee.

While performing the internal audit of subsequent year, Mr. ABC faces following situations. Please provide the course of action to be taken by Mr. ABC and points to be taken care in reporting the outcome of such procedures.

1. 2 High risk rated issues were not implemented by the process owners.
2. 2 medium risk rated issues were not implemented by the process owner, however the quantum of business transactions in these areas have reduced significantly.
3. 2 medium risk rated issues were not implemented by the process owner, however the quantum of business transactions in these areas have increased significantly.
4. Action plan to implement maker checker in 1 high risk issue pertaining to payroll function is not implemented however, the company has outsourced the payroll function to a third-party vendor.

Response 1: 2 High Risk rated issues were not implemented by the process owners

CIA must report the status of implementation and highlight such areas as critical risk requiring immediate attention of audit committee towards such areas. It is duty of the internal auditor to evaluate the applicability of such issues and whether the organization continue to be exposed to high business risk due to delay in implementation of such high-risk areas.

Response 2: 2 medium risk rated issues were not implemented by the process owner, however the quantum of business transactions in these areas has reduced significantly.

CIA must report the status of implementation to top management and audit committee. It is duty of the internal auditor to evaluate the applicability of such issues and whether the organization continue to be exposed to business risk due to delay in implementation of such medium risk areas. Reduced quantum of business transaction in such areas does not necessarily reduce the open risk for the company on account of past transaction. The auditor needs to evaluate the overall situation and must highlight the issues to audit committee in light of such analysis.

Response 3: 2 medium risk rated issues were not implemented by the process owner, however the quantum of business transactions in these areas have increased significantly.

CIA must report the status of implementation to top management and audit committee. It is duty of the internal auditor to evaluate the applicability of such issues and whether the organization continue to be exposed to business risk due to delay in implementation of such medium risk areas. Increase in quantum of business transaction in such areas clearly denotes the increase in risk and exposure of company due to open risk. Further, the auditor may also consider to increase the risk rating of such not implemented issues and evaluate the overall situation and must highlight the issues to audit committee in light of such analysis.

Response 4: Action plan to implement maker checker in 1 high risk issue pertaining to payroll function is not implemented however, the company has outsourced the payroll function to a third-party vendor.

It is duty of the internal auditor to evaluate the applicability of such issues in light of the changes process. The re-assessment is required for the risk to which the business is exposed and whether the alternate and compensating control is available to mitigate such risk in the changed process. The auditor must report the status of implementation to audit committee depending on the outcome of the revised assessment. If the risk is either not applicable in changed business process or the same is mitigated due to compensating controls, then the implemented status may be reported to audit committee to provide comfort and assurance; the gravity of open risk and status of not implemented should be reported to audit committee in other scenarios.

Project Closure

There are certain points which an Internal Auditor must ensure during project closure. Effective documentation and project closure is equally important to mitigate audit risk and establish good ground for subsequent audits. Some of the points which an internal auditor must keep in mind for effective closure are summarized below:

- **Process maps / narratives** – Internal Auditor must ensure that the process flow charts and narratives depicting the business and process understanding obtained must be prepared and documented. He may consider to mark the places where the significant process risks are observed for subsequent reference purpose.
- **Walkthrough documents** – Audit must perform business process and system walkthrough to see the way process is operated and not rely only on the verbal confirmation from the process owner. Appropriate documentation of such understanding must be maintained in the working paper file in the form of notes or screenshots.
- **Audit Plan** – Detailed audit plan and approach followed along with all consideration made to arrive at the plan must be documented in the working paper file.
- **Detailed Audit work plan including Risk and Controls Matrix** – Detailed audit work plan containing all identified risks, controls, audit checks performed, sample verified and outcome of such audit checks must be documented with evidence of review of audit supervisor and audit lead.
- **Document to support basis of sampling** – Internal Auditor should document the basis of sampling, population used for sampling and filtering criteria if any used for sampling.
- **Testing sheets** – Detailed testing sheet should be prepared and documented along with review notes and evidence. Such testing sheet may include the brief process summary, risk identified, existing controls noted on business understanding and walkthrough, Audit checks performed, population and sample used for each check, outcome of such testing and design and operating gap noted during the audit, management reporting timelines, management response and action plan agreed for each of the audit check performed.
- **Issue Sheets –** Detailed issue sheets should be retained and documented along with evidence of review. Refer section phase 4 for details to be documented in such issue sheets.
- **Evidence / document to support issues** – All audit evidence collected during the audit must be retained along with testing sheet and issue sheets. The same must be linked to audit checks and audit issues noted for easy reference.
- **Management Communication** – Evidence and trail of all important management communication must be retained in the working paper file.
- **Final report** – Internal auditor must ensure that all requirements of final report and circulation of such

reports is met. Copy of final report along with distribution list must be retained in the working paper file.

- **Points for consideration during next audit –** Any important points to be recalled during subsequent audit or notes for the other auditors must be mentioned in this section. E.g., any activity that could not be audited due to audit limitation or matter beyond control. Any new or emerging activity not audited due to low quantum of business transaction but needs to be evaluated in subsequent audit etc.

DOCUMENTATION

The auditor shall document:

- The overall audit strategy
- The audit plan
- Any significant changes made during the audit engagement to the overall audit strategy or the audit plan, and the reason for changes.

The documentation of overall audit strategy is a record of the key decision considered necessary to plan the audit and to communicate significant matters to the engagement teams.

The following should be a part of auditor's documentations:

- A summary of discussions with the entity's key decision makers.
- Documentation of Audit Committee pre-approval of services, where required.
- Other communication or arrangements with management or those charged with governance regarding the scope or changes in scope, of our services.
- Auditor's report on the entity's financial statements.
- Information gathered about the business and its operations, systems and processes and past or known issues.
- Audit Universe and summary of Auditable Units.
- Risk assessment documentation.
- Summary of available resources, their competencies and the proper matching of their skills with the audit requirements.
- Final overall internal audit plan, duly approved by the competent authorities.

AUDIT PROGRAMME

The internal auditor should also prepare a formal internal audit programme listing out the procedures essential for meeting the objective of the internal audit plan. Though the form and content of the audit programme would vary with the circumstances of each case, yet the internal audit programme should be so designed as to achieve the objectives of the engagement and also provide assurance that the internal audit is carried out in accordance with the Standards on Internal Audit.

The following points are taken mainly while making detailed planning:

a) Major observations pointed out in previous internal audit report and action taken by the auditee on these observations.

b) Checklist of previous audit assignment is also referred to get the insight about the areas to be focused in next assignment.

c) Any new changes / amendments taken place in commercial laws.

d) Any special area / investigation as instructed by the top management.

e) Results of various exception reports as run in ERP at head office before start of internal audit assignment.

The internal audit programme includes:

- the objectives of the internal audit in respect of each area,
- the staff responsible for carrying out the particular activity,
- the time allocated to each activity,
- detailed instructions to the staff as to how to carry out those procedures.

A well prepared, comprehensive audit programme helps proper execution of the work as well as proper supervision, direction and control of the performance of the engagement team.

The goal of an audit programme is to create a framework that is detailed enough for any outside auditor to understand what official examinations have been completed, what conclusions have been reached and what the reasoning is behind each conclusion. The framework should explain the audit's objectives, its scope and its timeline. The audit programme should also describe how working papers -- the documented evidence of the audit -- will be collected, reviewed and reported.

LESSON ROUND-UP

- Planning an audit involves:
  (a) Establishing the overall audit strategy
  (b) Developing an audit plan
- "The auditor should plan his work to enable him to conduct an effective audit in an efficient and timely manner. Plans should be based on knowledge of the client's business".
- A Typical internal audit engagement comprises of following five phases.

  Phase 1 – Obtain Business understanding

  Phase 2 – Plan Audit Engagement

  Phase 3 – Perform Audit Execution and Supervise Engagement

  Phase 4 – Communicate Engagement Results

  Phase 5 – Monitor Engagement Outcomes and Project Closure
- The auditor shall document:
  a) The overall audit strategy
  b) The audit plan
  c) Any significant changes made during the audit engagement to the overall audit strategy or the audit plan, and the reason for changes.

- The documentation of overall audit strategy is a record of the key decision considered necessary to plan the audit and to communicate significant matters to the engagement teams.
- Audit Programme: The internal auditor should also prepare a formal internal audit programme listing out the procedures essential for meeting the objective of the internal audit plan. Though the form and content of the audit programme would vary with the circumstances of each case, yet the internal audit programme should be so designed as to achieve the objectives of the engagement and also provide assurance that the internal audit is carried out in accordance with the Standards on Internal Audit.
- The internal audit programme includes:
    a) the objectives of the internal audit in respect of each area,
    b) the staff responsible for carrying out the particular activity,
    c) the time allocated to each activity,
    d) detailed instructions to the staff as to how to carry out those procedures.

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

1. Planning is not a discrete phase of an audit but rather a continual and iterative process? Discuss.
2. The nature, timing and extent of the direction and supervision of the audit team members and review of their work vary depending on many factors? Explain.
3. Is it necessary to document an audit plan? If so, what all activities in the planning phase needs to be documented?
4. List out the sources wherefrom the internal auditor can obtain such knowledge of the client's business.
5. What are the various advantages of Audit Planning?
6. Explain the various phases of Internal Audit Engagement.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Internal Audit Tools and Techniques

Lesson 5

KEY CONCEPTS

■ Data Gathering ■ Data Analysis ■ Work Papers ■ Permanent File ■ Current File ■ Sampling ■ Flowchart ■ Questionnaires

Learning Objectives

To understand:

- Data Gathering and its methods
- Data Analytics Techniques, Tools, and Usage in Audit
- The concepts of documentation, nature and purpose of documentation, Important aspects in Documentation, Form, content and extent of documentation, audit file, Type of File , Permanent File, Current File
- The need for working papers, ownership and custody of working papers, Guidelines for preparation of working papers, Documents Checklist
- Audit evidence, Sources of Audit evidence, sufficiency and appropriateness of audit evidence, types of audit evidence, relevance and reliability of audit evidence. The Importance of written representations and the objectives, External Confirmation and its relevance
- Internal Audit Techniques such as Vouching, Inquiry and Confirmation, Reconciliation, Testing, Physical Verification, Analytical Procedure, Computation, Flowchart, Observation
- Audit Sampling, Application of Audit Sampling Techniques, Sample Selection Methods, Sampling Risk, Evaluating Results of Audit Sampling
- Flowchart and Internal Control Questionnaire
- Audit in Automation Environment

Lesson Outline

- Data Gathering
- Data Analysis, Interpretation and Reporting
- Documentation / Work Papers
- Audit Evidence
- Process Mapping including Flowcharting
- Steps in evaluation and its techniques
- Use of Sampling Techniques and its tests
- Flowcharts and Internal Control Questionnaires
- Automation
- Lesson Round-Up
- Test Yourself
- List of Further Readings

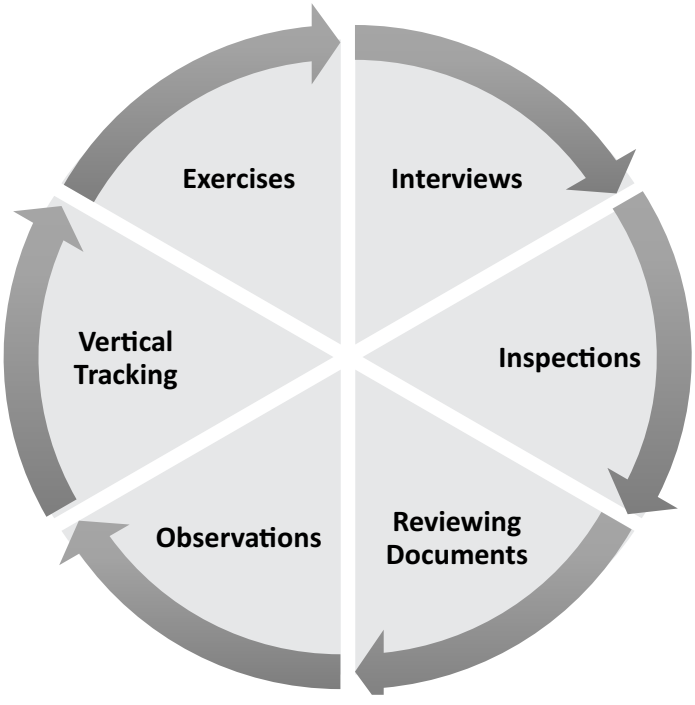
DATA GATHERING

Knowing how to look, where to look, and what to look for is the key to meeting the audit objectives. Therefore, data gathering is a big and highly important part of any internal audit. It is up to the Internal Auditor to decide which method or methods of collecting information to use for the audit and how to coordinate his or her actions with the auditee.

An Internal Auditor should always support his or her conclusions about an audit with information gathered by as many different methods as possible. Restricting oneself to only one viewpoint is unlikely to produce an accurate result. When a problem is found, it is important to dig deeper and identify the extent and the root cause of the problem.

Carrying out all the chosen data gathering tasks diligently will help the Internal Auditor conduct a successful audit.

There are six basic methods of gathering information during an audit. Depending on the type of information that needs to be obtained, the Internal Auditor will need to determine which method, or combination of methods, should be used.



(i) Interviews

Interviewing is a powerful data collection technique, which works well on its own and is often used to support other techniques, such as observation. The interviewee's insights can guide the Internal Auditor's decisions about what to observe. The most important thing to remember when interviewing is to always talk to the right person. It sounds obvious but talking to the person who has the information you need can save a lot of time and confusion. In addition, as an Internal Auditor, being prepared for interviews is vital. Having a list of questions ready in advance and using them to guide the interviewee through the discussion in a neutral way will result in an informative, constructive and positive discourse. Communication is a key element to the success of any audit. The more effectively the Internal Auditor interviews personnel, the more useful information will be gathered. The objective of an interview is to get the person to talk. Open-ended questions will allow the interviewee to demonstrate his or her understanding of the requirements,

procedures and show evidence of compliance. Questions may be asked several times in different ways or to different people depending on their level of responsibility (Operator, Supervisor, etc.) in order to get a complete answer.

Interviews are of two types: structured and unstructured (i.e., less structured). A structured interview is one in which auditors ask the same questions of numerous individuals or individuals representing numerous organizations in a precise manner, offering each interviewee the same set of possible responses. In contrast, an unstructured interview contains many open-ended questions that are not asked in a structured, precise manner. With unstructured interviews, different auditors interpret questions and often offer different explanations.

(ii) Inspections

When inspecting something, it is good practice to start with general observations and proceed to more specific elements. First, the Internal Auditor will have a good overall look around the facility and then examine specific items more closely, noting anything that does not seem quite right. It is important to ask questions throughout the inspection. The big picture must make sense and any detail that doesn't fall into place needs to be scrutinized. If a problem is found, the Internal Auditor must investigate (dig deeper) to explore the extent of the finding. This can involve looking at similar processes in other areas, talking to more people and checking more examples. The aim is to determine if this is an isolated case or a systemic problem, and if possible, the extent of the issue and any impact or potential impact on product.

(iii) Reviewing Documents

When reviewing company records, the Internal Auditor can use a number of techniques. Random sampling is one of them. It gives a general idea of the quality of record keeping and exposes the potential problem areas. However, one sample taken in one given period of time is usually not enough to form accurate conclusions. It may be more effective to check records based on a common characteristic that seems to be problematic and systemic. When reviewing documents, the Internal Auditor should check them for currency and validity. Another important aspect of record keeping is clarity. Documents should be clear regardless of who reads them. Details vary but, in general, every document should carry a title, an owner and a revision status. If any of this information is missing, the Internal Auditor should ask why. The revisions noted should be checked against the master record. Changes must be authorized, signed and dated by an authorized person.

(iv) Observations

The simplest way to check how a process works is to observe it in action. Observing a routine activity for a couple of hours can give the Internal Auditor opportunity to see how something is done under normal circumstances. He or she should ask questions about what they see, making sure at all times not to interfere with the processes they are observing, as that may cause the personnel not to carry out their tasks as they usually do.

(v) Vertical Tracking

This method, which is also referred to as "vertical auditing", consists of following a specific development from the beginning untill the end, simultaneously checking all the records that are produced in the process. Applying the vertical tracking technique can lead the Internal Auditor to areas that were not initially part of the scope, but it does facilitate a bigger picture view, as this allows the Internal Auditor to see how the various parts of a given program work together.

(vi) Exercises

The aim of an exercise is to test something that is usually done at the facility as part of the routine. However, the Internal Auditor gets to pick the time and the circumstances for the test. The subject of testing can be the

personnel, the program, or the equipment. An Internal Auditor should not run an exercise without the knowledge and cooperation of the auditee. Doing so is likely to have negative consequences as unannounced actions may breach certain facility-specific rules or regulations which the Internal Auditor is unaware of.

DATA ANALYTICS, INTERPRETATION AND REPORTING

Data Analytics may be defined as the science of examining raw data with the purpose of drawing conclusions about that information. This would involve the discovery, interpretation, and communication of meaningful patterns in data.

Auditors have been using data analytics to derive meaning or identify exceptions to the rules. However, data analytics approaches enable them to do more than just to identify exceptions or describe the data.

As a process, data analytics encompasses the process of accessing data, extracting data, preparing the data, using the data for analytics, carrying out various analysis to discover and interpret the patterns and relationships in the data.

By analyzing data from a variety of sources against control parameters, business rules, and policies, internal audit can provide fact-based assessments of how well automated controls are operating. It can also be used to determine if semi-automated or manual controls are being followed by seeking indicators in the data. By analyzing 100 percent of relevant transactions and comparing data from diverse sources, internal audit can identify instances of fraud, errors, inefficiencies, or non-compliance.

Techniques for Data Analytics

Data is presentation of facts or events in a numeric or representational form. Historically, the main forms of data to be analysed have been in numeric form. The text and image data (information) has been analysed manually. So have the audio or video data been analysed manually. Digitalisation has, now, made it possible to convert all kinds of information, text, image, video or audio, apart from the numerical data to be datafied, i.e., represented through a set of numerical dataset. This makes it possible to analyse and draw insights not only from numerical data but also text, image, audio and video datasets.

Statistics is the science of dealing with numeric data – collection, analysis, presentation and interpretation. It is also used to estimate about a population by analysis of a sample dataset drawn from the population.

Statistical Techniques

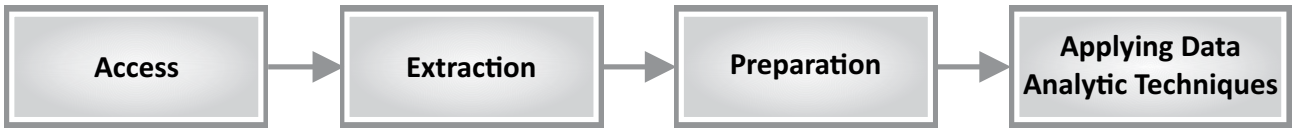
The most basic of the statistical techniques would be representing data in a simple tabular form and finding measures of central tendencies, viz, mean, median and mode. While interpreting the central tendencies, it is also important to have a measure of the spread or variance in the dataset, viz., standard deviation, variance, range, quartiles etc. These two measures are descriptive measures which describe the behaviour of the dataset and allow the auditor to make an estimate of the population characteristic from analysis of a sample dataset. When described over a period of time or along a class or geographically, these present a trend.

Visualisation Techniques

The results of statistical analysis can be better appreciated when they are visually presented. With the tools available today, visualisation in different forms is possible. Some of the visualisation techniques are the scatter plots, line plots, box plots, pie charts, vector plots, polar plots, bubble plots, heat maps etc.

Tools for Data Analytics

The data analytic process involves access to the datasets, extraction of datasets, preparation of the datasets, applying data analytic techniques and storing of the datasets and the results.



Access

The access to databases may be as per any of the modes such as:

- Manual Records
- Sharing the data on removable disk
- Read only rights in the audited entity systems
- Electronic transfer of data
- Cloud services – online data access
- Real time data sharing.

The tools should have the capacity to be able to access the datasets through any of these modes. Most tools available now a days are capable to access data through any of the modes available.

Extraction

The distinction between access and extraction needs to be understood wherein the extraction of data/ datasets means identifying and obtaining the relevant datasets for the purpose of analytics, whereas the access would refer to the access to the complete database from the auditee and also involves the physical transfer of the datasets from the auditee to the auditor's environment. The stage of extraction requires understanding of the datasets to identify the relevant datasets from the databases accessed and then extract them in the auditor's environment. This stage requires the data environment to be created at the auditor's end to be able to read the database. Further, the relevant datasets are extracted from the database by running appropriate queries. Most tools have connectors available to link to different database environments.

Preparation

While the extraction phase involves extracting the relevant datasets, the dataset may not be ready to be subjected to analysis as it may have missing values, null values, zero values, duplicates, gaps or outliers. These have the impact of distorting the picture derived from the data analysis. Further, there may be requirements to add two datasets through join or by appending them or even to split the dataset into two or more sets, as required. Undertaking activities to address the data deficiencies or to add or split datasets is what is called data preparation.

Applying data analytic techniques

The techniques described in the previous section are applied on the datasets through the use of algorithms built into the modern day analytic tools. It is the detail to which the tools have the capability to analyse that may distinguish them. While there are quite a few licensed tools available, many of the data analytic tools today are available as open source tools. It is for the auditor to decide on the usefulness of the tools keeping in mind the security of the data being handled through the tools as well as the sustainability, if the data analytic results are to be used repeatedly.

Usage of Data Analytics in Audit

The data analytics may be used in any of the stages of Audit – audit planning, audit execution, reporting. But, as can be clearly seen from the above discourse on use of techniques and tools, data analytics is useful in drawing

insights on the datasets. This makes data analytics useful for the audit planning phase. Audit planning involves setting of audit objectives, scope, methodology for audits. The insights on datasets can be used to decide on all of these. During the audit execution stage, data analytics can be useful in identifying exceptions, drilling down etc. At the reporting stage the data analytic results and the conclusions drawn from the audit process may be reported using appropriate visualisation techniques.

The patterns from the data analytics become important for auditors from the fact that trends and patterns have the potential of identifying unusual events, even though no rules are broken.

Conclusion

Data analytics has the potential to assist the Auditor in discharging his crucial role in providing assurance on the delivery of public services to the people of a country. It helps him in drawing insights and relevant conclusions about large and complex functions carried out by the entity. It assists him in deriving all relevant insights from the available information making the process of the audit more efficient and effective. Knowledge of data analytic process and techniques would play a crucial role in equipping the Auditor to deal with the intricacies present in datasets available.

DOCUMENTATION / WORK PAPERS

Meaning of Documentation

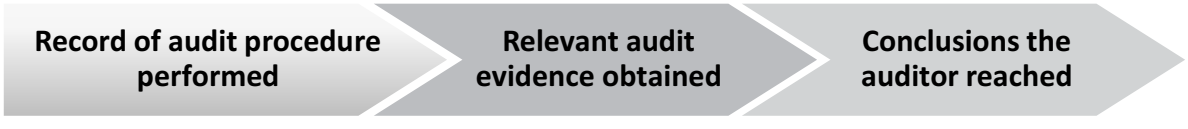
The word "document" is used to refer to a written or printed paper that bears the original, official, or legal form of something and can be used to furnish decisive evidence or information. "Documentation" refers to the act or an instance of the supplying of documents or supporting references or records.

"Documentation" refers to the working papers prepared or obtained by the auditor and retained by him, in connection with the performance of the audit.

SA 230 on "Audit Documentation", deals with the auditor's responsibility to prepare audit documentation for an audit of financial statements.

During the performance of the Internal Audit, the internal auditor also needs to report on the adequacy of systems and process in the company. The internal audit function greatly assists the other auditor like Secretarial Auditor and Statutory Auditor in determining the extent to which he can place reliance upon the work of the internal auditor.

Audit Documentation refers to the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached. (terms such as "working papers" or "work papers" are also sometimes used.)



The important aspects to be considered in this context are:

1. **Organisational Status** - Whether internal audit is undertaken by an outside agency or by an internal audit department within the entity itself. The internal auditor reports to the management, in an ideal situation he reports to the highest level of management and is free of any other operating responsibility. Any constraints or restrictions placed upon his work by management should be carefully evaluated. In particular, the internal auditor should be free to communicate fully with the external auditor.
2. **Scope of Audit Function** - The external auditor should ascertain the nature and depth of coverage of the assignment which the internal auditor discharges for management. He should also ascertain to what extent

the management considers, and where appropriate acts upon internal audit recommendations.

3. **Technical Competence** - The external auditor should ascertain that internal audit work is performed by persons having adequate technical training and proficiency. This may be accomplished by reviewing the experience and professional qualifications of the persons undertaking the internal audit work.

4. **Due Professional Care** - The external auditor should ascertain whether internal audit work appears to be properly planned, supervised, reviewed and documented. An example of the exercise of due professional care by the internal auditor is the existence of adequate audit manuals, audit programmes and working papers.

5. **Monitoring of internal control -** The internal audit function may be assigned specific responsibility for reviewing controls, monitoring their operation and recommending improvements thereto.

6. **Examination of financial and operating information -** The internal audit function may be assigned to review the means used to identify, measure, classify and report financial and operating information, and to make specific inquiry into individual items, including detailed testing of transactions, balances and procedures.

7. **Review of operating activities -** The internal audit function may be assigned to review the economy, efficiency and effectiveness of operating activities, including non- financial activities of an entity.

8. **Review of compliance with laws and regulations** - The internal audit function may be assigned to review compliance with laws, regulations and other external requirements, and with management policies and directives and other internal requirements.

9. **Risk management -** The internal audit function may assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.

10. **Governance -** The internal audit function may assess the governance process in its accomplishment of objectives on ethics and values, performance management and accountability, communicating risk and control information to appropriate areas of the organization and effectiveness of communication among those charged with governance, external and internal auditors, and management.

Illustration 1:

A new team member of the auditors of ABC Limited was of the view that Audit Documentation does not help in planning the audit of any company. Explain whether Audit Documentation has any relation with regard to planning the audit of a company?

Solution:

Audit Documentation helps in planning the audit of a company in a proper manner and also helps in conducting the audit of that company in a more effective way.

Form and content of Documentation

The form and content of audit documentation should be designed to meet the circumstances of the particular audit. The information contained in audit documentation constitutes the principal record of the work that the auditors have performed in accordance with standards and the conclusions that the auditors have reached. The quantity, type, and content of audit documentation are a matter of the auditors' professional judgment. The Audit documentation therefore is not restricted to being only on papers, but can also be on electronic media.

Generally the factors that determine the form and content of documentation for a particular engagement are:

(a) The nature of the engagement.

(b) The nature of the business activity of the client.

(c) The status of the client.

(d) Reporting format.

(e) Relevant legislations applicable to the client.

(f) Records maintained by the client.

(g) Internal controls in operation.

(h) Quality of audit assistants engaged in the particular assignment and the need to direct and supervise their work.

Audit File

Audit file may be defined as one or more folders or other storage media, in physical or electronic form, containing the records that comprise the audit documentation for a specific engagement.

Illustration 2:

While auditing the books of accounts of a company, a team member of the auditors was of the view that with regard to audit of the company, no relation exists between Audit File and Audit Documentation. Explain the relationship between Audit File and Audit Documentation

Solution:

Audit file may be defined as one or more folders or other storage media, in physical or electronic form, containing the records that comprise the audit documentation for a specific engagement. The auditor shall assemble the audit documentation in an audit file and complete the administrative process of assembling the final audit file on a timely basis after the date of the auditor's report.

Permanent and Current Audit files

In the case of recurring audits, some working paper files may be classified as permanent audit files, which are updated currently with information of continuing importance to succeeding audits. In contrast current audit files contain information relating primarily to the audit of a single period.

Content of permanent audit file

(a) Copy of initial appointment letter if the engagement is of recurring nature.

(b) Record of communication with the retiring auditor, if any, before acceptance of the appointment as auditor.

(c) NOC from previous auditor.

(d) Information concerning the legal and organisational structure of the entity. In the case of a company, this includes the Memorandum and Articles of Association. In the case of a statutory corporation, this includes the Act and Regulations under which the corporation functions, i.e.

  (i) In case of partnerships- Partnership deed.

  (ii) In case of trusts- Trust deed.

  (iii) In case of societies- Certificate of registration/ Rules and Bye-laws.

(e) Organisational structure of the client.

(f) List of governing body including Name, Address and contact details. For instance, the list of directors in case of a company, list of partners in a partnership and list of trustees in a trust.

(g) Extracts or copies of important legal documents, agreements and minutes relevant to the audit.

(h) A record of the study and evaluation of the internal controls related to the accounting system. This might be in the form of narrative descriptions, questionnaires or flow charts, or some combination thereof.

(i) Copies of audited financial statements for previous years.

(j) Analysis of significant ratios and trends.

(k) Copies of management letters issued by the auditor, if any.

(l) Notes regarding significant accounting policies.

(m) Significant audit observations of earlier years.

(n) Assessment of risks and risk management.

(o) Major policies related to Purchases and Sales.

(p) Details of sister concerns.

(q) Details of Bankers, Registrars, Lawyers, etc.

(r) Systems and Data Security policies.

(s) Business Continuity Plans.

Need for Audit Documentation

The audit working papers (current and permanent) for a client audit engagement should be sufficiently detailed to enable another appropriately experienced and competent auditor who is not familiar with the client to obtain an overall understanding of the engagement.

Need for Working papers

The need for Working papers listed as follows:

(a) They aid in the planning and performance of the audit;

(b) They aid in the supervision and review of the audit work and to review the quality of work performed, in accordance with AAS 17 “Quality Control for Audit Work”;

(c) They provide evidence of the audit work performed to support the auditor’s opinion;

(d) They document clearly and logically the schedule, results of test, etc.;

(e) The working papers should evidence compliance with technical standards;

(f) They document that Internal control has been appropriately studied and evaluated; and

(g) They document that the evidence obtained and procedures performed afford a reasonable basis for an opinion;

(h) They retain a record of matters of continuing significance to future audits of the entity;

(i) They enable an experienced auditor to conduct quality control reviews in accordance with Statement on Peer Review issued by the Institute of Chartered Accountants of India;

(j) The process of preparing sufficient audit documentation contributes to the quality of an audit;

(k) They fulfill the need to document oral discussions of significant matters and communicate to those charged with governance, as discussed in AAS 27, "Communication of Audit Matters with those Charged with Governance.

Retention of Working Papers/ Documents

The auditor should retain the working papers for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal or professional requirements of record retention.

Ownership and custody of Working Papers

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of or extracts from his working papers available to his client.

Illustration 3:

A director of a company was of the view that Audit Documentation of a company is the property of that company. Comment on the contention of the director regarding the audit documentation of the company?

Solution:

Audit Documentation of a company is not the property of the company rather Audit Documentation is the property of Auditor of that company.

General Guidelines for the preparation of Working Papers

The auditor should adopt reasonable procedures for custody and confidentiality of his working papers General guidelines for the preparation of working papers are:

1. **Clarity and Understanding** – As a preparer of audit documentation, step back and read your work objectively. Would it be clear to another auditor? Working papers should be clear and understandable without supplementary oral explanations. With the information the working papers reveal, a reviewer should be able to readily determine their purpose, the nature and scope of the work done and the preparer's conclusions.
2. **Completeness and Accuracy** – As a reviewer of documentation, if you have to ask the audit staff basic questions about the audit, the documentation probably does not really serve the purpose. Work papers should be complete, accurate, and support observations, testing, conclusions, and recommendations. They should also show the nature and scope of the work performed.
3. **Pertinence** – Limit the information in working papers to matters that are important and necessary to support the objectives and scope established for the assignment.
4. **Logical Arrangement** – File the working papers in a logical order.
5. **Legibility and Neatness –** Be neat in your work. Working papers should be legible and as neat as practical. Sloppy work papers may lose their worth as evidence. Crowding and writing between lines should be avoided by anticipating space needs and arranging the work papers before writing.
6. **Safety** – Keep your work papers safe and retrievable.
7. **Initial and Date** – Put your initials and date on every working paper.
8. **Summary of conclusions** – Summarize the results of work performed and identify the overall significance of any weaknesses or exceptions found.

Documents Checklist

S. No.	Particulars	Yes/No/ NA	Remarks/ Working Papers Ref
1.	Whether the audit documentation is prepared on a timely basis?		
2.	Whether the audit documentation is sufficient to enable an experienced auditor, having no previous connection with the audit, to understand the following? (a) The nature, timing, and extent of the audit procedures performed to comply with the SAs and applicable legal and regulatory requirements; (b) The results of the audit procedures performed, and the audit evidence obtained; and (c) Significant matters arising during the audit, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions.		
3.	While documenting the nature, timing and extent of audit procedures performed, whether the following was recorded (a) The identifying characteristics of the specific items or matters tested; (b) Who performed the audit work and the date such work was completed; and (c) Who reviewed the audit work performed and the date and extent of such review.		
4.	Whether the documentation includes discussions of significant matters with management, those charged with governance, and others, including the nature of the significant matters discussed and when and with whom the discussions took place.		
5.	Where it is identified that information is inconsistent with the auditor's final conclusion regarding a significant matter, whether it is documented as to how the inconsistency was addressed?		
6.	Where it is considered necessary in exceptional circumstances to depart from a relevant requirement in a SA, whether the audit documentation reflects how the alternative audit procedures performed achieved the aim of that requirement and the reasons for the departure.		

S. No.	*Particulars*	*Yes/No/ NA*	*Remarks/ Working Papers Ref*
7.	Where in exceptional circumstances, new or additional audit procedures are performed or new conclusions are reached after the date of the audit report, whether the following were documented? (a) The circumstances encountered; (b) The new or additional audit procedures performed, audit evidence obtained, and conclusions reached, and their effect on the auditor's report; and (c) When and by whom the resulting changes to audit documentation were made and reviewed.		
8.	Is it ensured that after the assembly of the final audit file has been completed, no deletion or discard of audit documentation of any nature has taken place before the end of its retention period?		
9.	Where it is necessary to modify existing audit documentation or add new audit documentation after the assembly of the final audit file has been completed, whether the following were documented? (a) The specific reasons for making them; and (b) When and by whom they were made and reviewed.		

Illustrative Working Paper Format

XYZ Limited	**Audit Firm's name**
Nature of Assignment	**Article Assistants name**
HO/Unit:	**For the period_____**
	Date of audit
	Reviewed by:
Area:	
Sub-area:	
Balance as per Balance Sheet:	
Balance as per General Ledger:	
Difference:	
Reason for difference if any:	
Checking Notes:	
Observations:	
Conclusions:	

AUDIT EVIDENCE

Audit evidence may be defined as the information used by the auditor in arriving at the conclusions on which the auditor's opinion is based. Audit evidence includes both information contained in the accounting records underlying the financial statements and other information.

Illustration 4:

Explain the relationship between Audit Evidence and Opinion of Auditor?

Solution:

There exists a very important relationship between Audit Evidence and opinion of the Auditor. While conducting an audit of a company, the auditor obtains audit evidence and with the help of that audit evidence obtained, the auditor forms an audit opinion on the financial statements of that company.

Characteristics of Evidence in an Audit

1. **Nature** refers to the type of information received. It can be received in many forms – presentations, orally, or through physical records.
2. **Relevance** refers to the pertinence of the information to provide an opinion.
3. **Reliability** refers to determining whether the material can be trusted or relied upon to form an opinion. The source of the information needs to be considered.
4. **Source** refers to whether the accounting evidence was obtained directly from the audited company or an external source. External source information is preferable since it is less subject to manipulation than internally sourced information.
5. **Sufficiency** refers to whether the information provided is enough to provide an opinion or make an accurate judgment.

Illustration 5:

Explain whether sufficiency and appropriateness of audit evidence mean simplicity and ease of obtaining audit evidence.

Solution:

Sufficiency and Appropriateness of audit evidence does not mean simplicity and ease of obtaining audit evidence rather sufficiency of audit evidence is related to the quantity of audit evidence and appropriateness of audit evidence is related to quality of audit evidence.

Sources of Audit Evidence

Some audit evidence is obtained by performing audit procedures to test the accounting records.

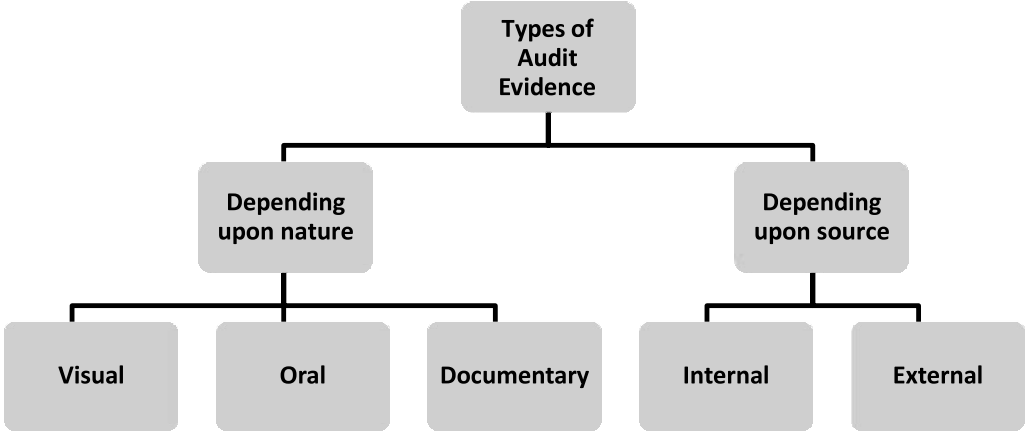
- through analysis and review,
- re-performing procedures followed in the financial reporting process,
- and reconciling related types and applications of the same information.

Through the performance of such audit procedures, the auditor may determine that the accounting records are internally consistent and agree to the financial statements. More assurance is ordinarily obtained from consistent audit evidence obtained from different sources or of a different nature than from items of audit evidence considered individually.

Example: Corroborating information obtained from a source independent of the entity may increase the assurance the auditor obtains from audit evidence that is generated internally, such as evidence existing within the accounting records, minutes of meetings, or a management representation.

Note: Information from sources independent of the entity that the auditor may use as audit evidence may include confirmations from third parties, analysts' reports, and comparable data about competitors.

Types of Audit Evidence



Depending upon nature:

1. **Visual:** For example, observing physical verification of inventory conducted by the client's staff.
2. **Oral:** For example, discussion with the management and various officers of the client.
3. **Documentary:** For example, fixed deposit certificate, loan agreement, sales bill etc.

Depending upon source:

1. **Internal Evidence:** Evidence which originates within the organisation being audited is internal evidence. Eg: received note, inspection report, copies of cash memo, debit and credit notes, etc.
2. **External evidence:** The evidence that originates outside the client's organization is external evidence. Eg: Purchase invoice, supplier's challan and forwarding note, debit notes and credit notes coming from parties, quotations, confirmations, etc.

Illustration 6:

Audit evidence obtained internally from within the company under audit are more appropriate from the reliability point of view as compared to audit evidence obtained externally. It is valid?

Solution:

Audit evidence obtained externally is more appropriate from reliability point of view as compared to those which are obtained internally. The reason that audit evidence obtained externally is more appropriate from the point of view of reliability is that there is a very low risk that they can be altered or changed.

Written Representations

SA 580- "Written Representations" deals with the auditor's responsibility to obtain written representations from management and, where appropriate, those charged with governance.

Written representations may be defined as a written statement by management provided to the auditor to confirm certain matters or to support other audit evidence. Written representations in this context do not include financial statements, the assertions therein, or supporting books and records.

Written representations are necessary information that the auditor requires in connection with the audit of the entity's financial statements. Accordingly, similar to responses to inquiries, written representations are audit evidence.

Although written representations provide necessary audit evidence, they do not provide sufficient appropriate audit evidence on their own about any of the matters with which they deal. Furthermore, the fact that management has provided reliable written representations does not affect the nature or extent of other audit evidence that the auditor obtains about the fulfillment of management's responsibilities, or about specific assertions.

Illustration 7:

Taking written representation from management instead of Banker's certificate in support of Fixed deposits is sufficient?

Solution:

Although written representations provide necessary audit evidence, they do not provide sufficient appropriate audit evidence on their own about any of the matters with which they deal. Furthermore, the fact that management has provided reliable written representations does not affect the nature or extent of other audit evidence that the auditor obtains about the fulfillment of management's responsibilities, or about specific assertions.

Applying the above to the given problem, the auditor would further request the management to provide him with the Banker's certificate in support of fixed deposits held by the company.

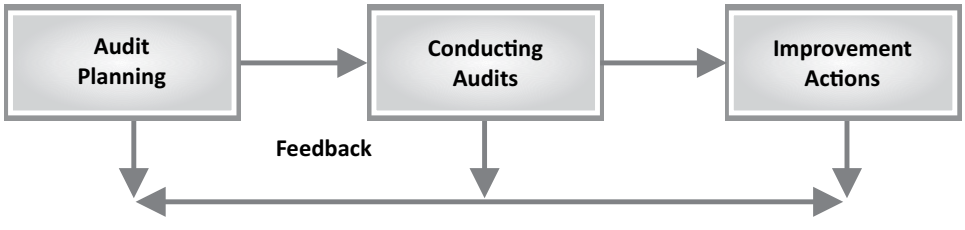
External Confirmation

SA 505- "External Confirmations", deals with the auditor's use of external confirmation procedures to obtain audit evidence.SA 500 indicates that the reliability of audit evidence is influenced by its source and by its nature, and is dependent on the individual circumstances under which it is obtained.

- Audit evidence is more reliable when it is obtained from independent sources outside the entity.
- Audit evidence obtained directly by the auditor is more reliable than audit evidence obtained indirectly or by inference.
- Audit evidence is more reliable when it exists in documentary form, whether paper, electronic or other medium.

PROCESS MAPPING INCLUDING FLOWCHARTING

Internal Audit Process



1. Establish and communicate the scope and objectives for the audit to appropriate management.
2. Develop an understanding of the business area under review. This includes objectives, measurements and key transaction types. This involves review of documents and interviews. Flow charts and narratives may be created if necessary.
3. Describe the key risks facing the business activities within the scope of the audit.

4. Identify control procedures used to ensure each key risk and transaction type is properly controlled and monitored.
5. Develop and execute a risk-based sampling and testing approach to determine whether the most important controls are operating as intended.
6. Report problems identified and negotiate action plans with management to address the problems.
7. Follow-up on reported findings at appropriate intervals. Internal audit departments maintain a follow-up database for this purpose.

STEPS IN EVALUATION AND ITS TECHNIQUES

AUDIT PLAN: An audit plan lays out the strategies to be followed to conduct an audit. It includes the nature, timing and extent of audit procedures to be performed by the team members. The auditor shall develop an audit plan while considering the following:

(a) The nature, timing and extent of planned risk assessment procedures.

(b) The nature, timing and extent of audit procedures at the assertion level.

(c) Other planned audit procedures that are required to be carried out so that the engagement complies with Standard on Auditing (SA).

INTERNAL AUDIT TECHNIQUES

Evidences are very important for an Auditor to form an opinion regarding financial statements. If Auditor fails to collect proper evidence, it will reduce the reliability of audit report. The method of collecting evidence is called audit technique.

An Internal auditor uses Internal Audit tools/techniques to ensure that controls, processes and policies are adequate and effective, and that they adhere to industry practices and regulatory mandates. An internal auditor also checks a corporation's financial statements to ensure that such reports are prepared in accordance with generally accepted accounting principles.

An auditor can apply various techniques of auditing which may be applied by the auditor under different circumstances of audit, the various techniques of the audit are summarised as under:

1. Vouching:

While verifying various transactions, the auditor examines the supporting documents and records. This technique is otherwise called vouching. The purpose of examining the documents and records is to confirm the authenticity (genuineness) of the transaction and :

- to find whether the transactions and the supporting document are appropriate.
- to ensure whether the transactions are authorized (approved).
- to ensure whether the classification of the transaction is proper.

While the scrutiny of documents, the auditor comes across the various records and documents and if he comes across any unusual transactions, he verifies the same thoroughly. This is called scanning of records, which requires experience and expertise. The auditor can rely on the documents depends on the origin (source) of the documents and the efficiency of the internal control system in operation. Also the written confirmation of the management of the company could be considered in case the supporting documents are not available.

Documents which have their origin in the hands of the third parties and held by third parties are more reliable than the documents which have their origin in the organization itself and held by the organization. One can classify the documents into four major categories according to their origin and availability.

a. Documents which have their origin in the hands of the third party and held by them – **Most reliable evidence**.

b. Documents which have their origin in the hands of the third party and held by the organization – **More reliable**.

c. Documents which have their origin in the hands of the organization and held by the third party – **Reliable**.

d. Documents which have the origin in the hands of the organization and held by the organization – **Reliable only if the internal control is effective**.

2. Inquiry and Confirmation

Inquiry: Seeking information from persons belonging to the organization or from outside organization is called inquiry. This method is used to collect in-depth information about any transaction.

Confirmation: Confirming the information available with the records of the organization or with the persons mostly from outside the organization through an inquiry is confirmation.

Inquiry and confirmation can take place either orally or in writing. The best example for inquiry and confirmation is confirming the balances of debtors shown in the accounting records with the debtors of the organization.

3. Reconciliation

Reconciliation is a technique used by an Auditor to know the reason of differences in balances. For example, to know the difference in the bank book of the client and the bank balance as appeared in the bank statement or pass book, the Auditor prepares the reconciliation statement. The same method may be used for debtors, creditors, etc.

4. Testing

Testing is a technique of selecting representative transactions out of whole accounting data to draw a conclusion about all items.

5. Physical Verification

If an item can be measured in physical term, the same may be verified for quantity and quality (if possible). By physical examination, the auditor can ensures the availability of the item. However, the ownership of the items cannot be verified through this method.

6. Analytical Procedures

The purpose of analysis is to ensure consistency of accounting methods and also to evaluate the efficiency of the management by comparing the results of several years. The several analytical procedures are Reconciliation, Ratio Analysis; and Variance Analysis. The auditor also applies the analytical procedures to help the management in decision making. Such analytical techniques are Marginal Costing, Standard costing etc.

7. Computation

An auditor makes appropriate calculations and verifies the accuracy of the accounting records. For example, the auditor computes the depreciation to be charged for the year, by taking into consideration, the value of the asset (cost), the date of purchase, the rate of depreciation, etc., to verify the accuracy of the depreciation charged by the organization. The auditor also traces a particular transaction from the origin to check the book keeping procedure.

8. Flow Chart

The Flow Chart technique is used by an Auditor to determine the stages of transaction and the generation of documents at all levels of transactions

9. Observation

The auditor observes a particular procedure being carried by the organization. Examples are observation of the internal control measures that are adopted in transactions involving cash, procedures followed on receipt or issue of material, etc. The auditor makes his observations to evaluate the efficiency and effectiveness of the system followed by the organization.

The auditor studies the nature of the business and also the prevailing circumstances and selects the techniques to be applied. While conducting the audit, he may change his technique according to the changes observed in the circumstances. The suitable audit techniques adopted by the auditor helps him to carry on the audit efficiently.

CASE STUDY

1. Company X was manufacturer of PVC. The finished product is in powder form and is sold in standard packaging of 25 kg bags. The bags are filled through an automated packing line and the quantity filled in bags is controlled through an online check weigher installed in the packaging line itself. In addition, tolerance limits were fixed for short/ excess filling in terms of number of grams per 25 kg bag. During the process review, the internal auditor carried out weighment of bags on a standalone weighing scale, selecting adequate sample and observed that in a large percentage of bags comprised in the sample, the actual quantity filled far exceeded the defined tolerance limits, i.e., 50 gms per 25 kg.

Functional head's response: This was only a statistical aberration and any such excess giveaways would get detected through other compensatory controls (manual) available like, random weighment of bags in a stand alone mode.

What should the Internal Auditor do in this situation?

Solution:

The internal auditor should co-ordinate with the commercial head and the warehouse in charge and took larger samples for study and validation of quantity bagged. In addition, the samples should be taken at different points of time. If, in all cases the results were consistent with the initial findings. By extrapolating the findings for over one year period, the quantity giveaways and cost implications (factoring both negative and positive variations) should be demonstrated to the functional head, along with live instances where the compensatory controls had failed to detect excess giveaways.

Accordingly, system based control viz., installation of check weighers in the conveyer, after filling level in the load cell should be recommend to introduced. This will result in to:

(i) Reduction of dependency to manual checking.

(ii) Increased accuracy level, since all bags are weighed after filling in load cell.

(iii) Reduction of labour in the filling and weighing section in the plant.

2. Company C started a Special Grade Fibre Manufacturing Plant for the first time in the country using imported technology. The products did not meet the quality parameters and were not accepted by the market, hence, the plant was closed down. The fiber intermediaries were left unused and not disposed for many years along with the imported chemicals and catalyst purchased for the manufacture of this product.

What should be the advice as an Internal Auditor in this situation?

Solution:

Internal auditors pointed out the situation with the suggestion that:

(i) the intermediary product may have market for fibre manufacturer and, therefore, classify as special product and dispose off.

(ii) the purchase orders for chemicals and catalyst should have the buy back clause so that the failed chemicals will be re-exported to the supplier at the pre-determined prices.

The process owners did not want to make any attempt to dispose off the intermediaries and the unutilised chemicals catalyst, stating that these materials do not have ready market.

Internal Auditor should follow-ups and persuasion with Research and Development Team of the company and identifies the possibility that the intermediaries can be sold to fibre manufacturers by sending sample and explaining the properties of the intermediaries. Further, the foreign vendors who supplied the chemical and catalyst should be given the left over chemicals sample and may be re-exported at appropriate price.

3. Internal auditor carried out a physical verification of Fixed Deposit Receipts on a surprise basis and tallied it with the Ledger balance. Finding no discrepancy the auditor submitted an assurance report. Finance head expressed the view that since this exercise was always carried out by the statutory auditors at the end of the year, this was a redundant exercise.

What should be the response of Internal Auditor in this situation?

Solution:

Internal auditor Response: Physical verification was done on a surprise basis to test that the controls are in place for custody of the Fixed Deposit Receipts and traceability rather than as a mere physical verification exercise. Since the controls were found to be in place an assurance report was issued by the internal auditor.

4. Company D manufactured polyester fibres. In manufacture of one grade of fibres, the company used old PET Bottles as a raw material. The PET bottles were procured in bulk and payment was made on the basis of weight stated in the invoice. On review of weight bridge data, the internal auditor observed major difference between the invoice weight and actual weight of material delivered. The process owners explained that the weight difference was on account of the moisture content in the material, which varies over time and evaporates during transit.

What should be the advice as an Internal Auditor in this situation?

Solution:

The internal auditor should highlight the weight difference together with the annualized financial implication to the management and insisted for fixing a tolerance limit of moisture content and to fix variable price based on the moisture content.

5. Company B was involved in manufacturing and selling of "paints". As per the routine procedure, physical verification of finished products was taken by the internal auditors in the mid of March so that the final report can be submitted before the year end. If any discrepancy is noticed it can be suitably adjusted in the books to give the correct financial statements. During the physical verification, certain discrepancies were noticed by the internal auditor and a draft report was submitted to the concerned functional head stating the differences noticed in the various ranges of the paint. On seeing the draft report, the functional head told his deputy to look into it and come back on the queries after completing his routine job. The deputy, therefore, gave last priority to the draft report. Internal auditor after 7 days of the issue of draft called upon the functional head to have a meeting so as to close out the report. Functional head during the telephonic discussion stated, "I have a lot of priority work to attend, for me sales is the most important activity. If we do not achieve our target the company is going to be under trouble and I do not want to inform the top management that I have been busy replying the Internal Audit Report. Any way what you are going to inform me has already happened isn't it? Audit is merely a post mortem job."

What should be the advice as an Internal Auditor in this situation?

Solution:

Internal Auditor should state that sales has to be accorded top priority, but if you come to know after taking the order that the actual stock is less you will not be able to honour your commitment and the customer will lose faith in you. Hence, request you to look at the actual stock figures and report".

6. Satyam Computers

B Ramalinga Raju, the founder of Satyam Computers, got into trouble after he admitted to inflating the company revenue, profit and profit margins for every single quarter over a period of 5 years, from 2003-2008. The amount misappropriated in this case is estimated to be around Rs. 7,200 crore.

In April 2015, Ramalinga Raju and his brothers were sentenced to 7 years in jail, and fined Rs. 5.5 crore.

Following are the common governance and audit problems, which have been noticed in the collapse of Satyam:

- **Unethical conduct** - Founders wanted to make money by avoiding paying taxes, cooking books, and pay offs; revealed some alarming truths that he was concealing for a long period by confessing to a fraud of Rs 7,800 crores ($1.47 billion) on Satyam's balance sheet.

- **A case of false books and bogus accounting** - These figures of accrued interest were shown in balance sheets in order to suppress the detection of such non-existent fixed deposits on account of inflated profits. The investigations also detailed that the company had deliberately paid taxes of about 186.91 crores on account of the non-existent accrued interests of Rs. 376 crores, which was a considerable loss for the company.
- **Unconvinced role of independent Directors** - The Satyam episode has brought out the failure of the present corporate governance structure that hinges on the independent directors, who are supposed to bring objectivity to the oversight function of the board and improve its effectiveness. They serve as watchdogs over management, which involves keeping their eyes and ears open at Board deliberations with critical eye raising queries when decisions scent wrong.
- **Questionable role of Audit Committee** - The true role of audit committee in précis is to ensure transparency in the company that financial disclosures and financial statements provide a correct, sufficient and creditable picture and that, cases of frauds, irregularities, failure of internal control system within the organization, were minimized, which the committee failed to carry out.
- **Dubious Role of Rating Agencies** - Credit rating agencies have been consistently accused of their lax attitude in assessing issuers and giving misleading ratings without thorough analysis they failed to warn market participants about the deteriorating condition of company.
- **Questionable Role of Banks** - While sanctioning short term loans why not the banks posed any question as to why the company which was supposedly cash rich as per the financial statements was taking loans from them.
- **Fake Audit** - The audit firm of Satyam have been auditing their accounts since 2000-01. The fraudulent role played by the Audit firm in the failure of Satyam. Partners of Audit Firm according to the SFIO findings had admitted they did not come across any case or instance of fraud by the company. However, founder admission of having fudged the accounts for several years put the role of these statutory auditors on the dock.

USE OF SAMPLING TECHNIQUES AND ITS TESTS

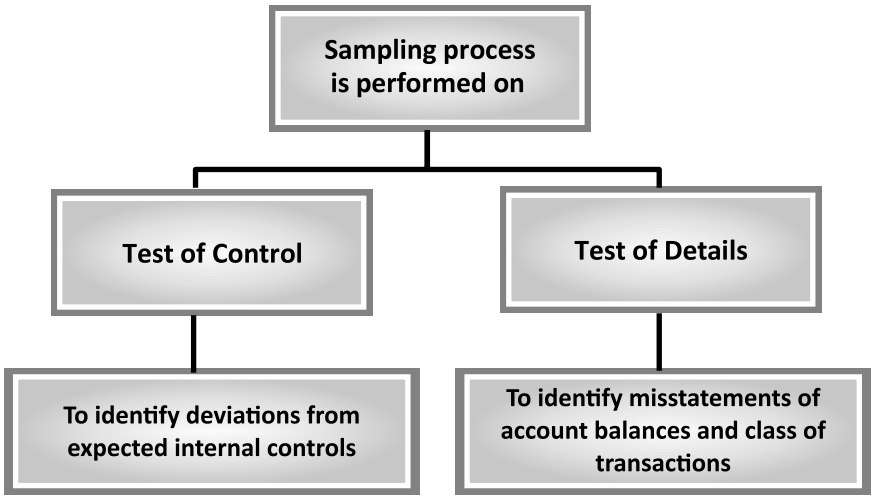
'Audit Sampling' refers to the application of audit procedures to less than 100% of items within a population relevant under the audit, such that all sampling units (i.e all the items in the population) have a equal chance of selection. This is to ensure that the items selected represent the entire population which enables the auditor to draw conclusions and express his opinion based on a pre-determined objective.

"Population refers to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions."

The auditor should select sample items in such a way that the sample can be expected to be representative of the population. This requires that all items in the population have an opportunity of being selected.

Sample must be representative

Whatever may be the approach non-statistical or statistical sampling, the sample must be representative. This means that it must be closely similar to the whole population although not necessarily exactly the same. The sample must be large enough to provide statistically meaningful results.



Audit sampling enables the auditor to obtain and evaluate audit evidence about some characteristic of the items selected in order to form or assist in forming a conclusion about the population, from which the sample is drawn. Audit sampling can be applied using either

- non-statistical or
- statistical sampling approaches.

Statistical sampling is an approach to sampling that has the random selection of the sample units; and the use of probability theory to evaluate sample results, including measurement of sampling risk characteristics.

Audit testing done through this approach is more scientific than testing based entirely on the auditor's own judgment because it involves use of mathematical laws of probability in determining the appropriate sample size in varying circumstances.

For Example: An auditor while verifying the Purchases during the year realised that the purchase transactions in that year are more than 45000 in number, then in such case, statistical sampling will be highly recommended in the audit program.

Non-statistical sampling is a sampling approach that does not have the above features's considered as **non-statistical sampling.**

For example, March, June and September may be selected in year one and different months would be selected in the next year, On basis of value of items, top 10 highest value. Etc.

An attempt would be made to avoid establishing a pattern of selection year after year, i.e the way of selecting samples, to maintain an element of surprise as to what the auditor is going to check.

Another fact about the sampling technique should be noted. It can never bring complete reliability; it cannot give precisely accurate results. It is a process of estimation. It may have some error. What error is tolerable for a particular matter under examination is a matter of the individual's judgment in that particular case.

Example: Mr. X may consider that in his estimation of stores valuation, an error of 2% may not be material; he also decides that he needs at least 98% reliability of the result. He is to pick up the requisite number of items of the stores for reliability of the result. The requisite number he can get from the random number table. The question of reliability of the result is directly linked with the reliability of the internal control and of the books and records; when these are satisfactory, lesser degree of reliability of the sampling estimation may suffice – if these are not satisfactory, the auditor may have to decide upon a higher degree of reliability which can only be obtained from a larger sample.

The factors that should be considered for deciding upon the extent of checking on a sampling plan are following:

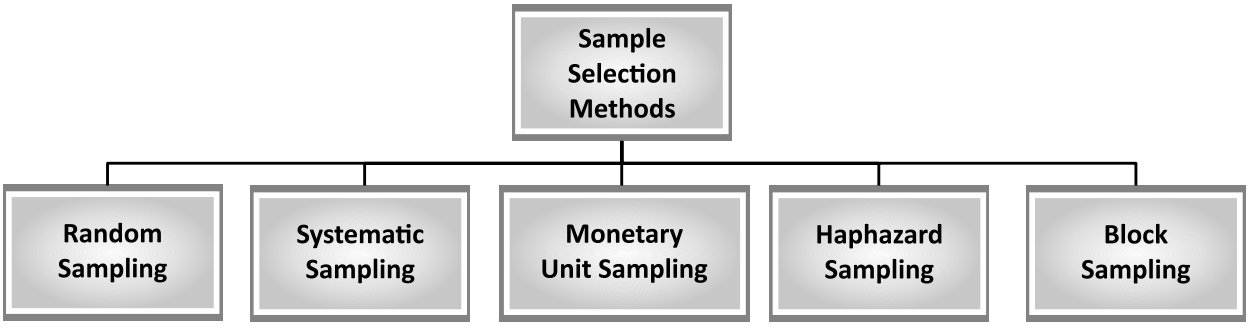
(i) Size of the organisation under audit.

(ii) State of the internal control.

(iii) Adequacy and reliability of books and records.

(iv) Tolerable error range.

(v) Degree of the desired confidence.



Random Sampling: Random selection ensures that all items in the population or within each stratum have a known chance of selection. It may involve use of random number tables. Each item in a population is selected by use of random number table either with a help of computer or picking up a number in a random way (may be randomly from a drum)

This method is considered appropriate provided the population to be sampled consists of reasonably similar units and fall within a reasonable range i.e. it is suitable for a homogeneous population having a similar range. **Example** The population can be considered homogeneous, if say, trade receivables balances fall within the range of Rs. 55,000 to Rs. 2,25,000 and not in the range between Rs. 525 to Rs. 10,50,000.

Stratified Sampling: This method involves dividing the whole population to be tested in a few separate groups called strata and taking a sample from each of them. Each stratum is treated as if it was a separate population and if proportionate of items are selected from each of these stratum.

Example 1: In the above case, trade receivables balances may be divided into four groups as follows:-

(a) balances in excess of Rs. 10,00,000;

(b) balances in the range of Rs. 7,75,001 to Rs. 10,00,000;

(c) balances in the range of Rs. 5,50,001 to Rs. 7,75,000;

(d) balances in the range of Rs. 2,25,001 to Rs. 5,50,000; and

(e) balances Rs. 2,25,000 and below

From these above groups the auditor may pick up different percentage of items from each of the group. From the top group i.e. balances in excess of Rs. 10,00,000, the auditor may examine all the items; from the second group 25% of the items; from the third group 10% of the items; and from the lowest group 2 per cent of the items may be selected. Random sample is chosen from each stratum using random number tables.

Systematic Sampling: Systematic selection is a selection method in which the number of sampling units in the population is divided by the sample size to give a sampling interval.

Example: If in a population of branch sales, particular branch sales occur only as every 100th item and the sampling interval selected is 100. The result would be that either the auditor would have selected all or none of the sales of that particular branch. If Accountant A is responsible to record all transaction in a particular month and Acountant B for next month ; if this structure is same throughout the year, and the auditor determines as his sample to check every transaction of alternate months, then only one accountant's work is checked by the auditor i.e. either Accountant A or B depending upon which month the checking started from. The work of other is overlooked and there could be a possibility of material misstatement in the transactions recorded by him. Therefore, systematic sampling when chosen as a method should be carefully applied to bring together every type of transaction within its purview. More than one starting point can be considered to minimize such risk.

Monetary Unit Sampling: It is a type of value-weighted selection in which sample size, selection and evaluation results in a conclusion in monetary amounts.

Haphazard sampling: Haphazard selection, in which the auditor selects the sample without following a structured technique. Although no structured technique is used, the auditor would nonetheless avoid any conscious bias or predictability (for example, avoiding difficult to locate items, or always choosing or avoiding the first or last entries on a page) and thus attempt to ensure that all items in the population have a chance of selection. Haphazard selection is not appropriate when using statistical sampling.

Block Sampling: This method involves selection of a block(s) of contiguous items from within the population. Block selection cannot ordinarily be used in audit sampling because most populations are structured such that items in a sequence can be expected to have similar characteristics to each other, but different characteristics from items elsewhere in the population.

Example: Take the first 200 sales invoices from the sales day book in the month of September; alternatively take any four blocks of 50 sales invoices. Therefore, once the first item in the block is selected, the rest of the block follows items to the completion.

Sampling Risk

The risk that the auditor's conclusion based on a sample may be different from the conclusion if the entire population were subjected to the same audit procedure. This risk will always be in existence when auditor uses sampling technique in conducting his audit.

IF THE ACCEPTABLE SAMPLING RISK IS LOW, LARGER SAMPLE SIZE IS NEEDED

Sampling risk can lead to two types of erroneous conclusions:

(i) In the case of a test of controls, that controls are more effective than they actually are, or in the case of a test of details, that a material misstatement does not exist when in fact it does. The auditor is primarily concerned with this type of erroneous conclusion because it affects audit effectiveness and is more likely to lead to an inappropriate audit opinion. This is because of over reliance on the internal controls.

(ii) In the case of a test of controls, that controls are less effective than they actually are, or in the case of a test of details, that a material misstatement exists when in fact it does not. This type of erroneous conclusion affects audit efficiency as it would usually lead to additional work to establish that initial conclusions were incorrect. This is because of under reliance on the test of controls and detailed substantive procedures performed by the auditor. Here risk of giving wrong opinion is minimum but it will lead to more detailed checking which is time consuming.

Risk of under relience on Test of Controls

↓

Risks of Incorrect rejection in substantive procedures

Leads to inefficiency in the conduct of audit

Risk of over relience on Test of Controls

↓

Risks of Incorrect acceptance in substantive procedures

Leads to erroneous audit opinion

Non-Sampling Risk The risk that the auditor reaches an erroneous conclusion for any reason not related to sampling risk.

Examples of non-sampling risk include use of inappropriate audit procedures, or misinterpretation of audit evidence and failure to recognize a misstatement or deviation.

CASE STUDY

In analyzing the deviations and misstatements identified, the auditor observed that many have a common feature, for example, type of transaction, location, product line or period of time. State the action point of Internal Audit in such situation?

Solution:

- The auditor may decide to identify all items in the population that possess the common feature, and extend audit procedures to those items. In addition, such deviations or misstatements may be intentional, and may indicate the possibility of fraud.
- Therefore, the auditor shall investigate the nature and causes of any deviations or misstatements identified, and evaluate their possible effect on the purpose of the audit procedure and on other areas of the audit.
- In the extremely rare circumstances when the auditor considers a misstatement or deviation discovered in a sample to be an anomaly, the auditor shall obtain a high degree of certainty that such misstatement or deviation is not representative of the population.
- The auditor shall obtain this degree of certainty by performing additional audit procedures to obtain sufficient appropriate audit evidence that the misstatement or deviation does not affect the remainder of the population.

Evaluating Results of Audit Sampling

The auditor shall evaluate-

a) The results of the sample; and

b) Whether the use of audit sampling has provided a reasonable basis for conclusions about the population that has been tested.

Illustration 7:

State with reasons (in short) whether the following statement is correct or incorrect:

i. The method which involves dividing the population into groups of items is knows as block sampling.

ii. Universe refers to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions.

iii. Non Statistical sampling is an approach to sampling that has the random selection of the sample items; and the use of probability theory to evaluate sample results, including measurement of sampling risk characteristics.

iv. Sample need not be representative.

v. The objective of stratification is to increase the variability of items within each stratum and therefore allow sample size to be reduced without increasing sampling risk.

vi. When statistical sampling is used to select a sample, sample need not be representative because the statistical sampling takes care of the representation.

vii. Stratified Sampling is used for homogeneous population.

viii. Non statistical sampling is considered to be more scientific than the statistical sampling.

ix. In case of Statistical sampling, auditor's bias in choosing sample is involved.

x. In stratified sampling, the conclusion drawn on each stratum can be directly projected to the whole population.

xi. Low acceptable sampling risk requires larger sample size.

Solution:

i. **Incorrect:** The method which involves dividing the population into groups of items is known as cluster sampling whereas block sampling involves the selection of a defined block of consecutive items.

ii. **Incorrect:** Population refers to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions.

iii. **Incorrect:** Statistical sampling is an approach to sampling that has the random selection of the sample items; and the use of probability theory to evaluate sample results, including measurement of sampling risk characteristics.

iv. **Incorrect:** Whatever may be the approach non-statistical or statistical sampling, the sample must be representative. This means that it must be closely similar to the whole population although not necessarily exactly the same. The sample must be large enough to provide statistically meaningful results.

v. **Incorrect:** The objective of stratification is to reduce the variability of items within each stratum and therefore allow sample size to be reduced without increasing sampling risk.

vi. **Incorrect:** Whatever may be the approach non-statistical or statistical sampling, the sample must be representative. This means that it must be closely similar to the whole population although not necessarily exactly the same. The sample must be large enough to provide statistically meaningful results.

vii. **Incorrect:** Stratified sampling is used when the population is diversified i.e heterogeneous. The population is divided into sub population having similar characteristics. Sample are then chosen from these sub populations which are called as Stratum. Therefore, stratified sampling is not useful in case of homogeneous population.

viii. **Incorrect:** Statistical sampling uses scientific method of choosing samples from a given population. The use of probability theory is involved in statistical sampling so that every sampling unit has an equal chance of getting selected. In the non statistical sampling, auditors' judgment and past experience is used to choose samples without any scientific method.

ix. **Incorrect:** Statistical sampling uses scientific method choosing samples from a given population. The use of probability theory is involved in statistical sampling so that every sampling unit has an equal chance of getting selected. In the non statistical sampling, auditor's judgment and past experience is used to choose samples without and scientific method. Hence, personal bias is involved in Non statistical sampling and not Statistical.

x. **Incorrect:** In case of stratified sampling, the conclusions are drawn on the stratum. The combination of all the conclusions on stratum together will be used to determine the possible effect of misstatement or deviation. Hence the samples are used to derive conclusion only on the respective stratum from where they are drawn and not the whole population.

xi. **Correct:** Sampling risk arises from possibility that the auditor's conclusion based upon sample may be different from conclusion that would have been reached if same audit procedures were applied on the entire population. If acceptable sampling risk is low, large sample size is needed.

FLOWCHARTS AND INTERNAL CONTROL QUESTIONNAIRES

Flow Chart

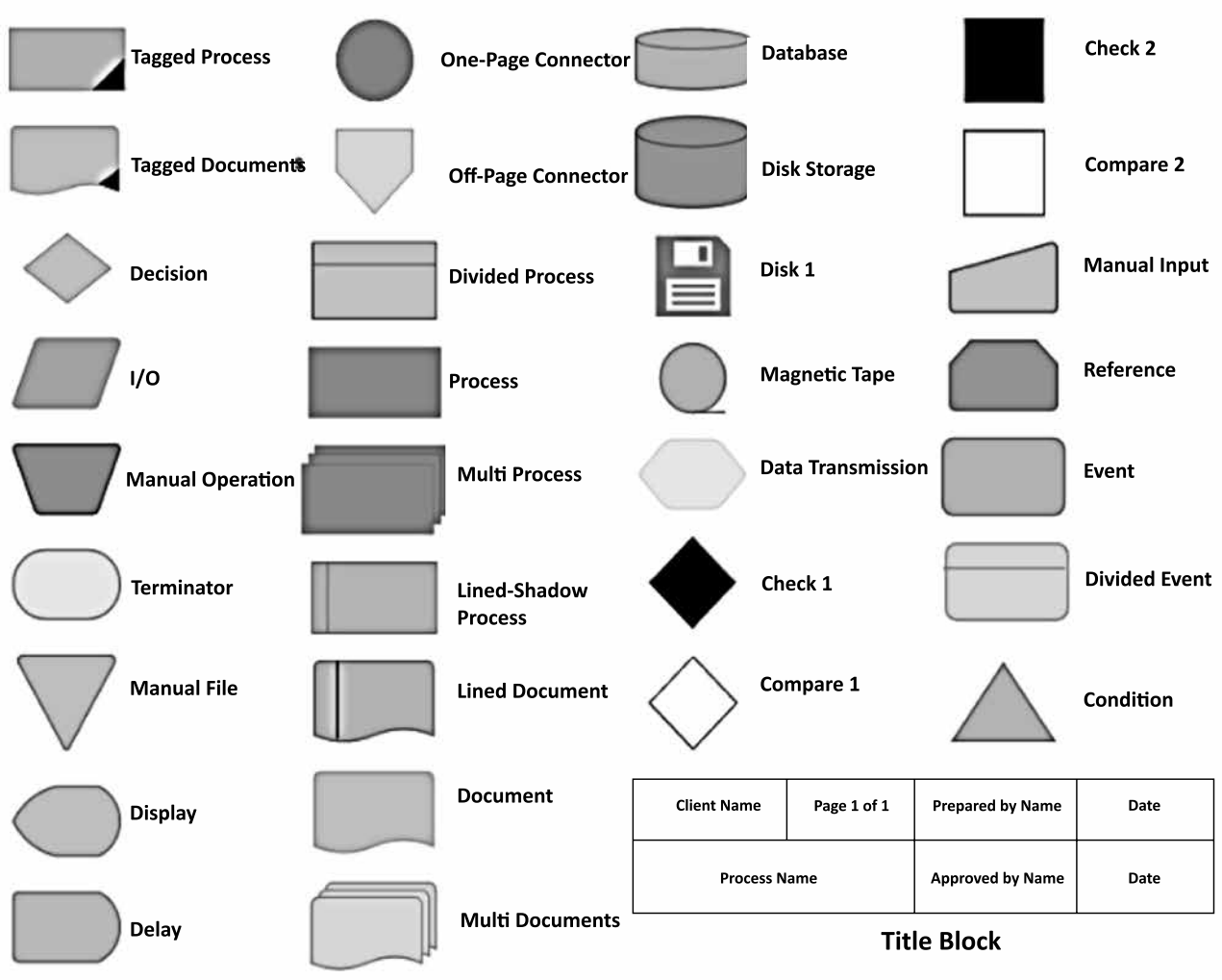
A flowchart is a type of diagram that illustrates workflows or different process from beginning to end and help attain the objectives of an internal auditing exercise. The flowchart symbols create visual clarity, thus allowing the viewers to follow through the stages of a process easier and without experiencing complications.

A well prepared flowchart would help in identifying the choke points in a business processes, the points of leakage or wastage of resources, highlight the important decision points in a business hierarchy, track the outcomes that flow from such avenues, and evaluate the efficacy of creating alternative points of decision. This is therefore not only useful for a specific audit activity but business managers and other stakeholders can also use these diagrams to track the flow of actions that drive a business. These flowcharts also enable business enterprises to create scope for process improvement and thus improve business outcomes. With ever increasing demand of Internal Auditors' assistance in fraud prevention, flowcharts could also be designed specifically to identify the scope of fraud inside a business process.

A flowchart is a type of diagram that represents a workflow or process. It shows the two most common items in a flow: Processing steps (as boxes) and Decisions (as diamonds). The order, or sequence, of the various activities, is shown by arrows and they are used to design, analyze, document and manage processes.

- Document Flowcharts, Showing Controls Over A Document-Flow Through A System
- Data Flowcharts, Showing Controls Over A Data-Flow In A System
- System Flowcharts, Showing Controls At A Physical Or Resource Level
- Program Flowchart, Showing The Controls In A Program Within A System

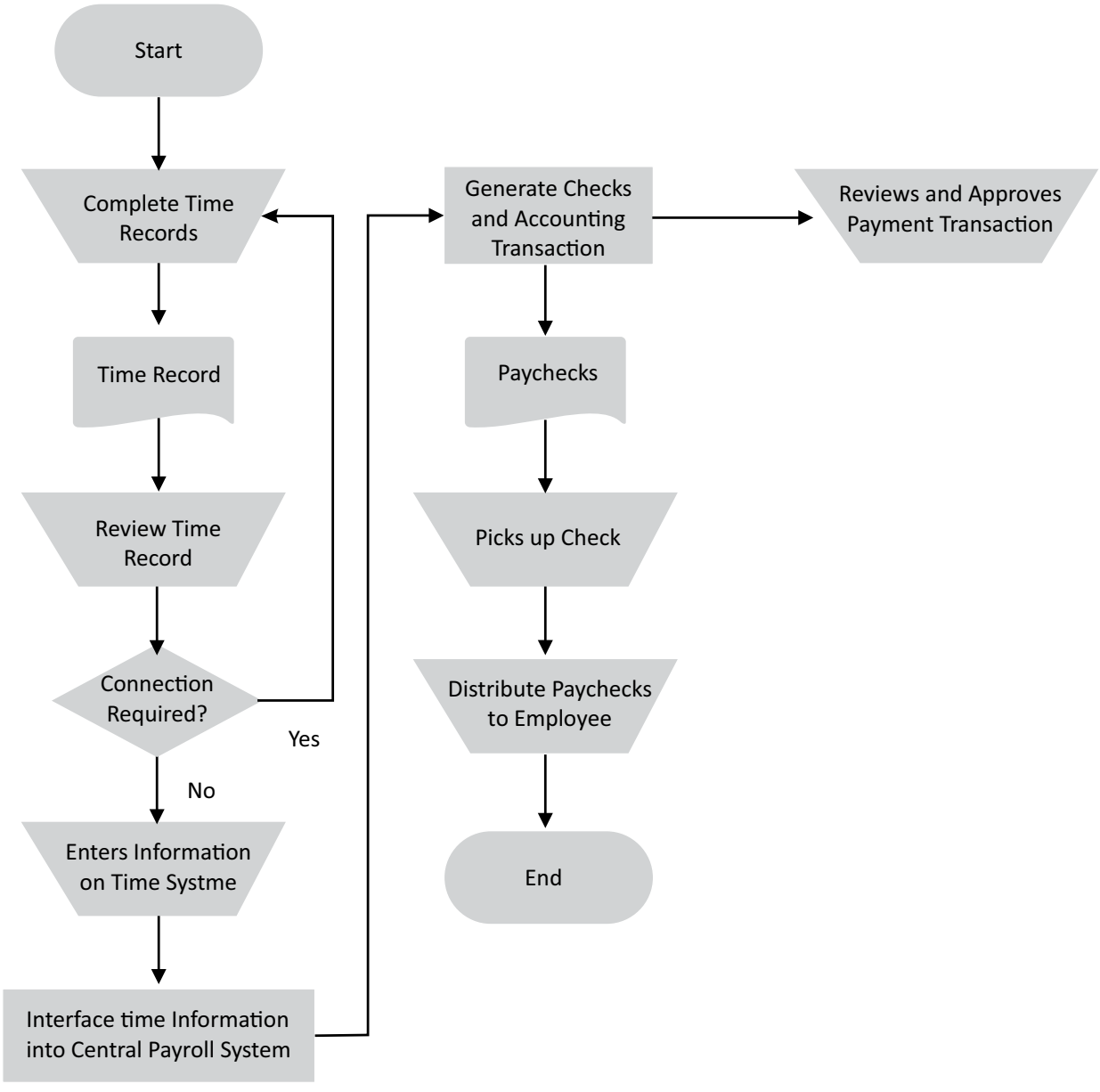
A flowchart for internal control and auditing consists of a mixture of elements from these four general types as follows:



Flowchart Example for Internal Control and Auditing – Payroll Function

The example below describes a Payroll function scenario using a flowchart for internal control purposes.

It starts from the felicitous employee "Joe" who complete the time record and submitted it to his supervisor, verified by Sven – the accountant and eventually issue a paycheck by Tami. Finally, the Summary payroll reports will be automatically generated by the system for internal auditing.



Internal Control Questionnaire

An internal control questionnaire is a document which an auditor provides to employees of a company before performing an audit. The questionnaire is useful to determine which areas the audit should focus on. When employees answer the questions, the auditor knows whether the company is keeping accurate records overall, and has evidence that shows who is responsible for which documents.

APPENDIX B

Internal Control Questionnaires – Instructions

This tool is designed to assist departments in identifying a project/work area for its Control Self-Assessment (CSA) Work Program.

If the department has already identified a specific project or function for review, consult with Internal Audit staff to assess the specific controls of that activity.

1. Determine which area or areas present the most risk or would offer the most benefit from a control self-assessment for your department.

   Internal Control Questionnaires (ICQs) are provided in the following areas (refer to each worksheet in this Excel file):

   - General Internal Controls
   - Finance - Cash
   - Finance - Revenue and Accounts Receivable
   - Finance - Expenditures and Accounts Payable
   - Expense Reports
   - County Properties & Fixed Assets
   - Payroll
   - Legal and Program Requirements
   - Information Systems

   Brief descriptions of each work area are provided in the header of most worksheets.

   The content in each worksheet/category may not address a work process that is unique to your department. In this case, review the questions in the worksheet to help you hone in on an area you'd like to review.

2. Once an area has been identified for your CSA, answer each question in the relevant sheet(s). Only complete the worksheets most relevant to your CSA.

3. Provide an explanation for each "no" response in the designated boxes.

4. Once all relevant worksheets have been completed, if there is more than one "no" response, determine the area that presents the highest risk to your department. The area of highest risk should be the focus of your Control Self-Assessment Work Program.

5. Refer to the Control Self-Assessment Work Program (Appendix A) for information on completing your CSA.

Questionnaire - General Internal Controls

The "General Internal Controls" questionnaire addresses the overall tone and operations of a department/ agency. General internal controls set the stage for how work is conducted.

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	GENERAL INTERNAL CONTROLS	***YES***	***NO***	***NOT SURE***	***N/A***
1.	Are the organization's mission, goals and objectives clearly defined in writing?				

2.	Are the organization's mission, goals and objectives communicated to all employees?				
3.	Are the operating and accounting policies, procedures, budgets, organizational charts, accounting manulas, chart of accounts, policy directives and memoranda etc. properly documented?				
4.	Does your department have an Ethics Policy and/or Code of Conduct?				
5.	Are year-to-date revenues and expenditures monitoried by upper management and periodically compared to budgeted amounts?				
6.	Are confidential records stored in secure areas with access to a limited number of employees?				
7.	Is a record retention policy in place to ensure that records are retained in accordance with legal and audit requirements?				
8.	Do employees receive adequate training to perform their duties?				
9.	Does management evaluate employee performance regularly and hold individuals accountable for their internal control responsibilities?				
10.	Are there procedures for employees to report unusual activity, or a mechanism to anonymously report suspicions of fraud?				
11.	Are internal controls in place to achieve objectives and respond to risks?				
12.	Are internal control monitoring activities in place, with a process in place to evaluate results?				
13.	Have there been any recent changes to any of the following areas: – Regulatory or operating environment – Management personnel – Information systems – Expansion of operations – New technology				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Finance - Cash

The questions in the "Finance" module are best answered by a manager(s) who is familiar with all aspects of department's financial operations.

"Cash" includes currencies (coins, Treasury notes, banknotes), checks, money orders and other legal tender of the United States. The subsections under "Cash" include "General", "Cash Collections", "Cash Disbursements" and "Petty Cash Funds and Change Funds". Answer the questions in the sections that are applicable and/or are known high risks for your department.

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	GENERAL	***YES***	***NO***	***NOT SURE***	***N/A***
1.	Is each revolving fund, trust fund and bank account established pursuant to specific written authorization by the Board of Supervisors, the County Treasurer and/or the County Auditor-Controller?				
2.	Is formal responsibility for each fund (including signature authority) vested in a specific County official(s)?				
3.	Are revolving funds, trust funds, and bank accounts reconciled to their accountable balances on a regular basis? Are the reconciliations performed or reviewed by a high level official?				
4.	Are cash overages and shortages identified, reported and corrected on a timely basis?				
5.	Is cash (including currency, coin, checks, money orders, etc.) physically safeguarded from theft and fraud?				
6.	Are cash losses reported to the District Attorney, Auditor-Controller and the County Risk Manager in accordance with the Manual of Accounting Policies and Procedures (MAPP), issued by the Auditor-Controller's Office?				

Provide an explanation for each "no" response under "General-Finance-Cash". Indicate the question # for which you are referring:

	CASH COLLECTIONS	***YES***	***NO***	***NOT SURE***	***N/A***
7.	Are the following duties performed by separate individuals? • Receipting • Posting • Depositing • Reconciling				

	CASH COLLECTIONS	YES	NO	NOT SURE	N/A
8.	Are all cash collections recorded immediately when received on pre-numbered receipt forms, cash register tapes and/or mail logs?				
9.	Does the information on the receipt include: date, amount, payer, method of payment, purpose of payment, cashier's name and account distribution?				
10.	Are the original copies of voided receipts marked "void," attached to the other copies of the receipt and retained for audit purposes?				
11.	Are checks restrictively endorsed immediately when received?				
12.	Are mail remittances listed immediately when received?				
13.	Are unidentified mail remittances promptly returned to the payer or deposited into a suspense account for further research?				
14.	Are collections transmitted promptly and intact by branch offices to the central office? Are the branch collections recorded on a batch transmittal log and slip? Are the transmitted amounts logged in, counted, reconciled and receipted by the central office, and are all variances or discrepancies immediately investigated?				
15.	Are controls in place to ensure that cash collections are not co-mingled with other funds, except change funds?				
16.	Is cash counted and reconciled to accountability (undeposited receipts and change funds) at the end of each shift?				
17.	Are cash overages and shortages properly accounted for, and are shortages replenished from a cash difference fund rather than offset against overages?				
18.	Are collections properly recorded, classified and summarized in a cash receipts journal?				
19.	Are collections deposited intact and on a daily basis into the County Treasury or a bank account authorized by the Board of Supervisors, the County Treasurer and/or the County Auditor-Controller?				
20	Are deposits and collections reported to the Auditor's Office on the monthly deposit register?				
21.	Are deposits and collections verified to the appropriate Alcolink accounts on a regular basis?				
22.	Are receipts physically inventoried and accounted for on a periodic basis?				

	CASH COLLECTIONS	YES	NO	NOT SURE	N/A
23.	Is the cashing of personal checks from County funds and cash collections prohibited?				
24.	Is a Board-approved fee levied on all returned checks?				
25.	Is cash on-hand and in-transit safeguarded from theft and fraud?				

Provide an explanation for each "no" response under "Cash Collections". Indicate the question # for which you are referring:

	CASH DISBURSEMENTS	YES	NO	NOT SURE	N/A
26.	Are the following duties performed by separate individuals? • Preparing vouchers/checks • Approving vouchers/authorizing disbursements • Reconciling disbursements • Maintaining custody of cash				
27.	Are disbursements made only from authorized expenditure accounts, trust funds, revolving funds or bank accounts and, except for petty cash payments, paid only through online vouchers, pre-numbered warrants/ checks, and/or journal entries?				
28.	Are controls in place to ensure that all disbursements are reasonable, necessary and made in accordance with state and federal regulations and County polices (as defined in the MAPP, MOUs, County Administrative Code, letter orders, OMB Circular A-87, etc.)?				
29.	Are cash advances prohibited except as authorized under special circumstances by the Board of Supervisors?				
30.	Are all disbursements supported by properly approved, original vendor invoices, employee claims, and/or contractor invoices and, if appropriate, contracts, purchase orders and receiving reports?				
31.	Are controls in place to ensure that only authorized personnel approve vouchers and sign warrants/checks?				
32.	Do voucher approvers or check/warrant signers review the supporting documentation before approving the voucher or signing the check?				

	CASH DISBURSEMENTS	YES	NO	NOT SURE	N/A
33.	Are all disbursements properly recorded, classified and summarized in a cash disbursements journal?				
34.	Are warrants and checks mailed out immediately after proofing and signing and not returned to the persons who prepared or approved them?				
35.	Are adequate controls maintained over unused, returned and voided checks/warrants and signature stamps, plates and files?				

Provide an explanation for each "no" response under "Cash Disbursements". Indicate the question # for which you are referring:

	PETTY CASH FUNDS AND CHANGE FUNDS	YES	NO	NOT SURE	N/A
36.	Are procedures for the use of petty cash funds clearly established and do they include: ● Clear definitions of authorized uses, including restrictions on the amount and type of disbursements? ● Prior approval of disbursements? ● Reimbursement only upon submission of receipt and/or other supporting documentation? ● Cancellation of voucher and supporting documentation? ● Timely replenishment of the fund?				
37.	Are controls in place to ensure that petty cash funds are not co-mingled with cash collections and other funds?				
38.	Are petty cash funds and change funds counted and reconciled to their accountable balances on a regular basis? Are the reconciliations performed or reviewed by someone other than the custodians of the funds?				
39.	Are cash funds counted and verified on a surprise basis by a supervisor?				
40.	Are overages/shortages identified, reported and corrected on a timely basis, and are shortages not offset or netted against overages?				

Provide an explanation for each "no" response under "Petty Cash Funds and Change Funds". Indicate the question # for which you are referring:

Questionnaire - Finance - Revenue and Accounts Receivable

The questions in the "Finance" module are best answered by a manager(s) who is familiar with all aspects of department's financial operations.

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	REVENUES AND ACCOUNTS RECEIVABLE	***YES***	***NO***	***NOT SURE***	***N/A***
1.	Are the following duties performed by separate individuals? • Providing services • Preparing billings • Approving billings • Receiving payments • Posting, adjusting and reconciling accounts				
2.	To the maximum extent possible, is revenue from all eligible sources identified, recorded and collected?				
3.	Are billings generated in a timely manner for all services rendered, goods sold and costs incurred?				
4.	Are all billings promptly recorded as accounts receivable?				
5.	Are authorized fee schedules used for all goods and services?				
6.	Are billing rates and service fees reviewed periodically to ensure that all costs, including indirect costs, are recovered to the maximum extent possible?				
7.	Are invoices pre-numbered and accounted for?				
8.	Are statements of accounts regularly sent to all debtors?				
9.	Are billings checked for accuracy before mailing?				
10.	Are the outstanding balances of individual accounts receivable summarized and reconciled to the control balances on a regular basis?				
11.	Are credits and refunds approved by an appropriate level of authority?				
12.	Is an aged trial balance (i.e., a listing of receivables grouped by age: 0-30 days, 31-60 days, 60 - 90 days, over 90 days) prepared on a regular basis to evaluate the adequacy of the collection process and to identify old, unpaid accounts which should be pursued for collection or written-off?				

13.	Are overdue accounts pursued for collection and, if appropriate, referred to Central Collections or other collection agencies?				
14.	Are uncollectible accounts identified and submitted to the Board of Supervisors on an annual basis for discharge from accountability?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Finance - Expenditures and Accounts Payable

The questions in the "Finance" module are best answered by a manager(s) who is familiar with all aspects of department's financial operations.

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

EXPENDITURES AND ACCOUNTS PAYABLE		***YES***	***NO***	***NOT SURE***	***N/A***
1.	Are the following duties performed by separate individuals? • Receiving goods • Preparing vouchers or checks • Approving vouchers and/or authorizing disbursements • Posting adjustments and reconciling accounts				
2.	Are procedures in place to ensure that all liabilities represent valid obligations and that all obligations are properly authorized, supported, recorded and classified?				
3.	Are expenditures made only from authorized budgetary accounts, trust funds, revolving funds or bank accounts and only through online vouchers, pre-numbered warrants/ checks, and/or journal entries?				
4.	Are controls in place to ensure that all expenditures are reasonable, necessary and made in accordance with state and federal regulations and County polices (as defined in the MAPP, MOUs, County Administrative Code, letter orders, OMS Circular A-87, etc.)?				
5.	Are procedures in place to ensure goods and services are obtained at competitive prices?				
6.	Are all payments and obligations based on properly approved, original vendor invoices, receipts, employee claims, or contractor invoices, and, as appropriate, contracts, purchase orders, receiving reports or other valid payment authorization?				

	EXPENDITURES AND ACCOUNTS PAYABLE	YES	NO	NOT SURE	N/A
7.	Do voucher approvers review the supporting documentation before approving the voucher?				
8.	Are invoices checked for mathematical accuracy and matched with purchase orders and receiving reports prior to payment?				
9.	Are controls in place to ensure that all available vendor discounts are taken, that cash flow is maximized and that vendors are paid on a timely basis?				
10.	Are individual accounts payable summarized and reconciled to control balances on a regular basis?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Expense Reports

The questions in the "Expense Reports" module are best answered by a manager(s) who is familiar with all aspects of department's financial operations.

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	EXPENSE REPORTS	YES	NO	NOT SURE	N/A
1.	Does your department require original receipts for all expenses claimed?				
2.	Does your department have any internal control to detect duplicate expenses in the absence of original receipts?				
3.	Are allowable expenses clearly explained in your department's policies and procedures?				
4.	Do certain expenses require pre-approval? If so, are they clearly outlined in your departmental policy? Are the pre-approvals documented and enforced?				
5.	Are there allowable expenses that need to be more clearly defined and/or need to be more restrictive(than the policies imposed by MAPP)?				
6.	Are expenses submitted for reimbursement in a timely manner? Do guidelines prescribe any deadline for submission? Does the department ensure that expenses are posted in Alcolink in their proper fiscal year?				

	EXPENSE REPORTS	YES	NO	NOT SURE	N/A
7.	Are expense reports reviewed by a supervisor or independent person prior to reimbursement?				
8.	For how long are expense reports and all supporting documentation retained?				
9.	Does your departmental policy define the consequences of fraudulent submissions?				
10.	Is proper justification provided for expenses, before they are incurred?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Properties & Fixed Assets

Properties include such non-monetary and non-digital assets as land, buildings & fixtures, furniture and equipment that are owned or leased. For practical purposes only items with estimated value at 5,000 or above are considered. Computers are considered under "Information Systems".

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	PROPERTIES & FIXED ASSETS	YES	NO	NOT SURE	N/A
1.	Are the following duties performed by separate individuals? ● Authorizing fixed asset acquisitions, transfers, and disposals ● Posting, adjusting and reconciling fixed asset records ● Maintaining custody and using fixed assets ● Taking inventory of fixed assets and reconciling to accountable balances				
2.	Are written policies and procedures in place regarding the acquisition, capitalization, depreciation, physical inventorying, transfer to salvage and discharge from accountability of fixed assets?				
3.	Are capital acquisitions authorized at an appropriate level of authority and in conformity with prescribed polices?				
4.	Are adequate detailed records of fixed assets maintained, including identification numbers, locations, descriptions, original cost and, if appropriate, accumulated depreciation?				

	PROPERTIES & FIXED ASSETS	YES	NO	NOT SURE	N/A
5.	Is a regular maintenance schedule followed to maintain the usefulness and value of the assets?				
6.	Is inventory taken on fixed assets and reconciled to their accountable balances on a regular basis?				
7.	Are dispositions and transfers of fixed assets authorized and made in conformity with prescribed policies?				
8.	Are fixed assets physically safeguarded from theft, fraud and misuse?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Payroll

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	PAYROLL	YES	NO	NOT SURE	N/A
1.	Are the following duties performed by separate individuals? ● Authorization of changes in payroll status (hiring, promotion, termination) ● Approval of timesheets ● Data entry of payroll information ● Distribution of payroll warrants ● Reconciliation of payroll records				
2.	Are written personnel and payroll policies and procedures in place regarding job descriptions and classifications, hiring, promotion, termination, timekeeping, salary rates, MOU provisions?				
3.	Are changes in employee status (hiring, promotion, termination) approved at an appropriate level of management and do the changes conform to established policies and procedures?				
4.	Is authorizing documentation on file for each employee regarding the employee's appointment, job classification, salary rate and step, proof of citizenship and required documentation?				

	PAYROLL	YES	NO	NOT SURE	N/A
5.	Are controls over employee timekeeping adequate? Specifically: ● Are all employees required to prepare and sign time sheets? ● Are time sheets reviewed and signed by the immediate supervisor? ● Are leaves of absence (vacation, sick leave) approved by the immediate supervisor? ● Is overtime authorized at an appropriate level of authority?				
6.	Where appropriate, is employee time documented in sufficient detail so that salaries can be properly allocated to programs and functions within the organization?				
7.	Are payroll warrants reviewed prior to distribution by an appropriate level of management to ensure that they are reasonable and accurate and that no unauthorized changes have been made?				
8.	Are payroll warrants distributed by someone other than the employees who prepared or input the payroll information?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Legal and Program Requirements

Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons. Provide an explanation for each "no" response.

	LEGAL AND PROGRAM REQUIREMENTS	YES	NO	NOT SURE	N/A
1.	Has the organization established procedures to ensure that all legal and program requirements are identified and complied with?				
2.	Does the organization periodically evaluate the efficiency, economy and effectiveness with which its program goals and objectives are achieved?				
3.	Are official bonds and insurance policies adequate for the needs of the organization and, where appropriate, have they been submitted to the County Risk Manager for review?				
4.	Are procedures in place to ensure that revenue from all eligible sources is properly identified, billed and collected?				

	LEGAL AND PROGRAM REQUIREMENTS	YES	NO	NOT SURE	N/A
5.	Does the organization have controls in place to ensure that subrecipients of federal, state and County funds are monitored on a regular basis to ensure compliance with contracts, grant agreements, the Single Audit Act, policy and procedures and other requirements from the funding sources?				
6.	Does the agency/entity have procedures in place to ensure that subrecipients which receive federal funds comply with general and specific federal program requirements, including: ● Political activity ● Prevailing wages ● Civil rights ● Cash management ● Federal financial reporting ● Cost principles ● Matching ● Eligibility ● Specific program requirements				
7.	Are all required financial reports submitted in a timely manner adhering to required deadlines?				
8.	Are procedures in place to ensure that questioned costs and other reported audit findings are reviewed and corrected in a timely manner?				
9.	Does the organization have policies and procedures in place to ensure that persons are not discriminated against on the basis of race, color, national origin, age, handicap, sex or religion?				
10.	Does the organization have policies and procedures in place to ensure a drug-free workplace?				
11.	Does the organization have policies and procedures in place to ensure a safe and secure workplace?				
12.	Does the organization have policies and procedures in place to ensure a workplace free of sexual harassment?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

Questionnaire - Information Systems

The questions in the "Information Systems" module are best answered by a manager(s) who is familiar with all aspects of information systems/technology.

The subsections under "Information Systems" include "Computer Equipment", "Protection of Information", and "Usefulness of

Information". Answer the questions in the sections that are applicable and/or are known high risks for your department. Answers must be based on observed facts, analyses or statements made by knowledgeable and reliable persons.

Provide an explanation for each "no" response.

	COMPUTER EQUIPMENT	***YES***	***NO***	***NOT SURE***	***N/A***
1.	Is the Countywide Computer Use Policy adopted and implemented?				
2.	Are policies specific to work units developed to protect equipment?				
3.	Is physical access to equipment limited to authorized personnel?				
4.	Are instructions and training provided to new equipment users?				
5.	Is equipment breakdown promptly reported and acted on?				
6.	Are purchases of equipment coordinated and planned to ensure long-term compatibility?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

	PROTECTION OF INFORMATION	***YES***	***NO***	***NOT SURE***	***N/A***
7.	Is a person designated as security administrator to ensure the security of information?				
8.	Is access to data and program files restricted to authorized personnel?				
9.	Is access to sensitive electronic information restricted by password?				
10.	Are procedures established for the retention and back up of critical computer files?				
11.	Is there a policy to control the risks from internet usage?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

	USEFULNESS OF INFORMATION	YES	NO	NOT SURE	N/A
12.	Is the usefulness of outpur from information systems periodically evaluated?				
13.	Are users periodically surveyed as to the usefulness of the information they receive?				
14.	Are users kept informed of new capabilities of the system?				

Provide an explanation for each "no" response above. Indicate the question # for which you are referring:

AUTOMATION

Let us first understand what the term "Automated Environment" means. An automated environment basically refers to a business environment where the processes, operations, accounting and even decisions are carried out by using computer systems – also known as Information Systems (IS) or Information Technology (IT) systems. Nowadays, it is very common to see computer systems being used in almost every type of business.

Think about how banking transactions are carried out using ATMs (Automated Teller Machines), or how tickets can be purchased using "apps" on mobile phones, etc. In these examples, you can see how these computer systems enable us to transact business at any time and any day.

Key features of an Automated Environment

i. Enabling faster business operation

ii. Accuracy in data processing and computation

iii. Ability to process large volume of transactions

iv. Better security and controls

v. Less prone to human errors

vi. Provides latest information

While it is true that the use of IT systems and automation benefit the business by making operations more accurate, reliable, effective and efficient, such systems also introduce certain new risks, including IT specific risks, which need to be considered, assessed and addressed by management. To the extent that it is relevant to an audit of financial statements, even auditors are required to understand, assess and respond to such risks that arise from the use of IT systems.

Given below are some situations in which IT will be relevant to an audit

- Increased use of Systems and Application software in Business (for example, use of ERPs).
- Complexity of transactions has increased (multiple systems, network of systems).
- Hi-tech nature of business (Telecom, e-Commerce).
- Volume of transactions are high (Insurance, Banking, Railways ticketing).
- Company Policy (Compliance).

In some of the above situations it is likely that carrying out audit using traditional substantive audit procedures may be difficult or even not feasible if the company prepares, records and conducts majority of business activities through IT systems only.

Another area where IT can be relevant to audit is by using data analytics using computer assisted audit techniques (CAATs). By using data analytics, it is possible to improve the effectiveness and efficiency of an audit.

Data Analytics for Audit

In today's digital age when companies rely on more and more on IT systems and networks to operate business, the amount of data and information that exists in these systems is enormous. A famous businessman recently said, "Data is the new Oil".

The combination of processes, tools and techniques that are used to tap vast amounts of electronic data to obtain meaningful information is called data analytics. While it is true that companies can benefit immensely from the use of data analytics in terms of increased profitability, better customer service, gaining competitive advantage, more efficient operations, etc., even auditors can make use of similar tools and techniques in the audit process and obtain good results. The tools and techniques that auditors use in applying the principles of data analytics are known as Computer Assisted Auditing Techniques or CAATs in short.

Data analytics can be used in testing of electronic records and data residing in IT systems using spreadsheets and specialised audit tools viz., IDEA and ACL to perform the following:

- Check completeness of data and population that is used in either test of controls or substantive audit tests.
- Selection of audit samples – random sampling, systematic sampling.
- Re-computation of balances – reconstruction of trial balance from transaction data.
- Re-performance of mathematical calculations – depreciation, bank interest calculation.
- Analysis of journal entries
- Fraud investigation
- Evaluating impact of control deficiencies.

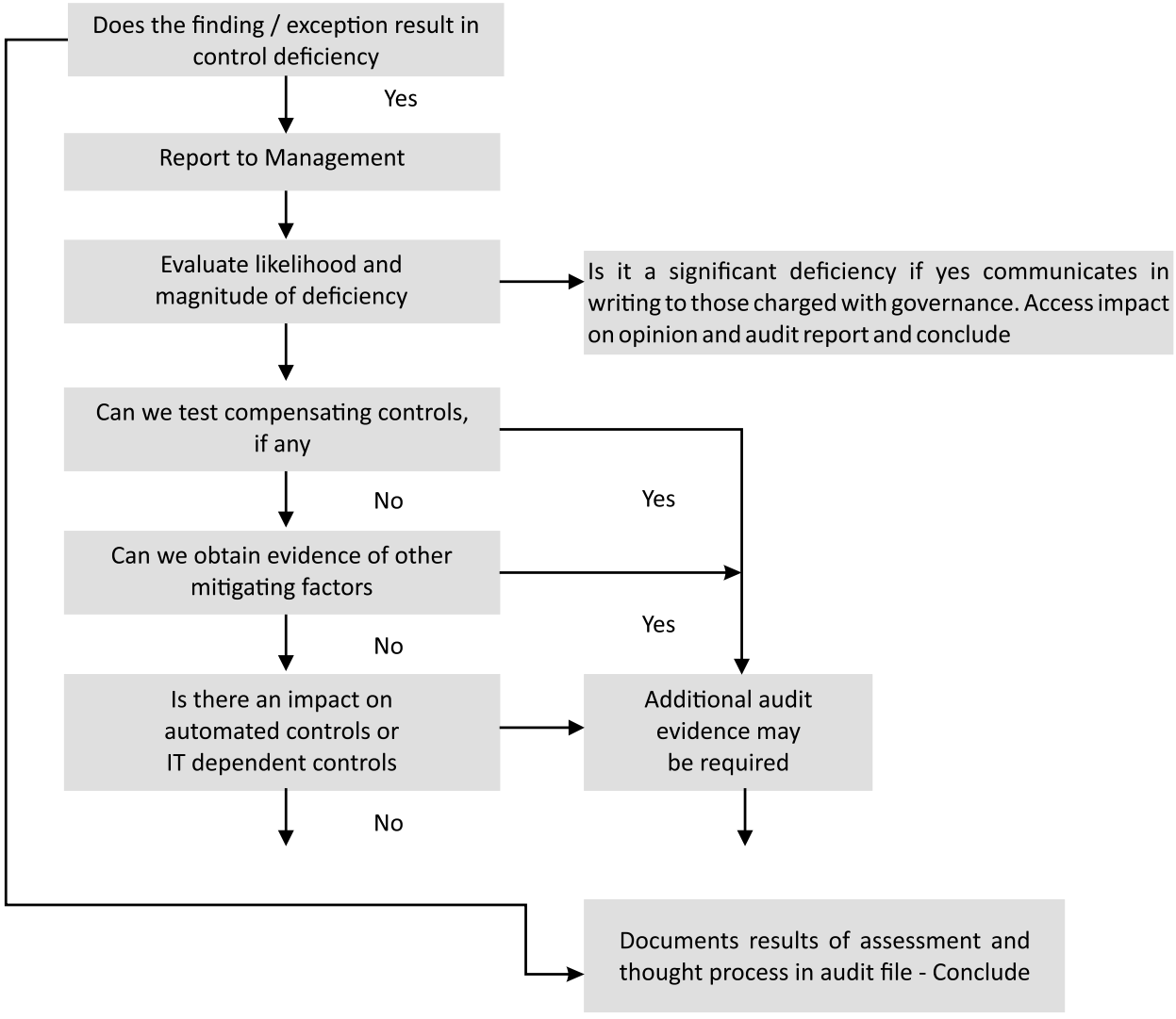
Assess and Report Audit Findings

At the conclusion of each audit, it is possible that there will be certain findings or exceptions in IT environment and IT controls of the company that need to be assessed and reported to relevant stakeholders including management and those charged with governance viz., Board of directors, Audit committee. Some points to consider are as follows:

- Are there any weaknesses in IT controls?
- What is the impact of these weaknesses on overall audit?
- Report deficiencies to management – Internal Controls Memo or Management Letter.
- Communicate in writing any significant deficiencies to Those Charged with Governance.

The auditor needs to assess each finding or exception to determine impact on the audit and evaluate if the exception results in a deficiency in internal control. Refer to the flowchart to learn how this assessment should be carried out. This approach and thought process is the same when auditing in an automated environment or when auditing in a more manual environment.

An approach to access audit findings



A deficiency in internal control exits if a control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or the control is missing.

Evaluation and assessment of audit findings and control deficiencies involves applying professional judgement that include considerations for quantitative and qualitative measures. Each finding should be looked at individually and in the aggregate by combining with other findings/deficiencies.

LESSON ROUND-UP

- An Internal Auditor should always support his or her conclusions about an audit with information gathered by as many different methods as possible.
- There are six basic methods of gathering information during an audit. Depending on the type of information that needs to be obtained, the Internal Auditor will need to determine which method, or combination of methods, should be used.

a) Interviewing

b) Inspection

c) Reviewing Documents

d) Observation

e) Vertical thinking

f) Exercises.

- **Data Analytics** may be defined as the science of examining raw data with the purpose of drawing conclusions about that information. This would involve the discovery, interpretation, and communication of meaningful patterns in data.
- The **data analytic** process involves access to the datasets, extraction of datasets, preparation of the datasets, applying data analytic techniques and storing of the datasets and the results.
- "**Documentation**" refers to the working papers prepared or obtained by the auditor and retained by him, in connection with the performance of the audit**. SA 230 on "Audit Documentation",** deals with the auditor's responsibility to prepare audit documentation for an audit of financial statements.
- **Audit file** may be defined as one or more folders or other storage media, in physical or electronic form, containing the records that comprise the audit documentation for a specific engagement.
- The auditor should retain the working papers for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal or professional requirements of record retention.
- Working papers are the property of the auditor. The auditor may, at his discretion, make portions of or extracts from his working papers available to his client.
- **Audit evidence** may be defined as the information used by the auditor in arriving at the conclusions on which the auditor's opinion is based. Audit evidence includes both information contained in the accounting records underlying the financial statements and other information.
- **Types of Audit Evidence**

  Depending upon nature:

  1. Visual: For example, observing physical verification of inventory conducted by the client's staff.
  2. Oral: For example, discussion with the management and various officers of the client.
  3. Documentary: For example, fixed deposit certificate, loan agreement, sales bill etc.

  Depending upon source:

  1. Internal Evidence: Evidence which originates within the organisation being audited is internal evidence. Eg: received note, inspection report, copies of cash memo, debit and credit notes, etc.
  2. External evidence: The evidence that originates outside the client's organization is external evidence. Eg: Purchase invoice, supplier's challan and forwarding note, debit notes and credit notes coming from parties, quotations, confirmations, etc.
- **SA 580- "Written Representations**" deals with the auditor's responsibility to obtain written representations from management and, where appropriate, those charged with governance.

- **SA 505- "External Confirmations",** deals with the auditor's use of external confirmation procedures to obtain audit evidence. SA 500 indicates that the reliability of audit evidence is influenced by its source and by its nature, and is dependent on the individual circumstances under which it is obtained.
- An Internal auditor uses **Internal Audit tools/techniques** to ensure that controls, processes and policies are adequate and effective, and that they adhere to industry practices and regulatory mandates. An internal auditor also checks a corporation's financial statements to ensure that such reports are prepared in accordance with generally accepted accounting principles.
- **'Audit Sampling'** refers to the application of audit procedures to less than 100% of items within a population relevant under the audit, such that all sampling units (i.e. all the items in the population) have a equal chance of selection. This is to ensure that the items selected represent the entire population which enables the auditor to draw conclusions and express his opinion based on a pre-determined objective.
- **"Population refers** to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions."
- **A flowchart** is a type of diagram that illustrates workflows or different process from beginning to end and help attain the objectives of an internal auditing exercise. The flowchart symbols create visual clarity, thus allowing the viewers to follow through the stages of a process easier and without experiencing complications.
- **An internal control questionnaire** is a document which an auditor provides to employees of a company before performing an audit. The questionnaire is useful to determine which areas the audit should focus on. When employees answer the questions, the auditor knows whether the company is keeping accurate records overall, and has evidence that shows who is responsible for which documents.

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

Correct/Incorrect

State with reasons (in short) whether the following statements are correct or incorrect:

1. "Audit Documentation", the working papers are not the property of the auditor.
2. Purchase invoice is an example of internal evidence.
3. Sufficiency is the measure of the quality of audit evidence.
4. Inquiry alone is sufficient to test the operating effectiveness of controls.

Answer:

1. *Incorrect*: As per SA 230 on "Audit Documentation" the working papers are the property of the auditor and the auditor has right to retain them. He may at his discretion can make available working papers to his client. The auditor should retain them long enough to meet the needs of his practice and legal or professional requirement.
2. *Incorrect*: Internal evidence is the evidence that originates within the client's organisation. Since purchase invoice originates outside the client's organisation, therefore, it is an example of external evidence.

3. Incorrect: Sufficiency is the measure of the quantity of audit evidence. On the other hand, appropriateness is the measure of the quality of audit evidence.
4. Incorrect: Inquiry along with other audit procedures (for example observation, inspection, external confirmation etc.) would only enable the auditor to test the operating effectiveness of controls. Inquiry alone is not sufficient to test the operating effectiveness of controls

Practice Question:

1. Explain audit documentation along with example.
2. "Although written representations provide necessary audit evidence yet they do not provide sufficient appropriate audit evidence on their own about any of the matters with which they deal". Discuss.
3. Explain stating clearly objectives of the auditor regarding written representation.
4. Most of the auditor's work in forming the auditor's opinion consists of obtaining and evaluating audit evidence. Explain.
5. What is meant by sufficiency of Audit Evidence?
6. What is the meaning of Sampling? Also discuss the methods of Sampling.
7. Explain the factors to be considered while determining the extent of checking on a sampling plan.
8. What precautions should be taken by the auditor while applying test check techniques?

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Internal Audit of Specific Functions

Lesson 6

KEY CONCEPTS

■ Kick-off Meeting ■ Process Walkthrough(s)

Learning Objectives

To understand:

- The process or activity that are critical to the various functions / department such as Purchase functions, Inventory management, production, operations, finance functions, human resource, Sales, Marketing & IT Functions etc.
- The process / steps / majors areas to be looked into by the internal auditor while conducting audit of such functions / department

Lesson Outline

INTRODUCTION

In the previous lesson, we have studied about internal audit tools and techniques, and how they can be used effectively while conducting an internal audit. In this lesson we take the discussion forward and learn about nuances of conducting internal audit of some specific functions or processes which are usually part of most of the organisations. We will strive to understand the practical aspects as well the possible risks and controls which may be audited in such audits. We will cover below internal audits in this lesson:

A. Internal Audit of Purchasing Activity,

B. Internal Audit of Inventory Management,

C. Internal Audit of Production and Operations,

D. Internal Audit of Finance and Accounts,

E. Internal Audit of Human Resources,

F. Internal Audit of Sales & Marketing,

G. IT System Audit.

Before we start discussing about specific audits as listed above, it is important to revisit the steps or stages of a typical internal audit engagement, since an understanding of these internal audit process milestones shall be helpful in better comprehension and application of the audit steps explained later on for the specific topics mentioned in this lesson.

Initiation of Internal Audit

An internal audit engagement generally starts with an audit notification being sent by the Internal Auditor to the relevant stakeholders. Generally, these stakeholders are Business Unit or Function or Vertical Heads (by whatever name called in the organisation), the senior management stakeholders including the relevant wholetime directors and other key managerial personnel identified by the company.

The objective of issuing an audit notification is to apprise the key stakeholders about the start of audit, the audit objectives and scope as approved by the audit committee or the board, as applicable and share the tentative schedule of the audit. It ensures that the senior people in the organisation are aware about the importance and schedule of the internal audit activity and can direct their subordinates to re-prioritise their tasks to enable smooth sharing of explanations, information and records to the internal audit team in a timely manner.

An audit notification generally contains a proposal to have kick-off meeting (sometimes called as information meeting), with the function owners, their immediate sub-ordinates who are the process owners of the items given in audit scope and audit co-ordinator (s) from the auditee / client side, if any.

Kick-off Meeting

After the audit notification is issued on email by the internal auditor, a kick-off meeting is generally organized by the internal auditor with the relevant function owners and their subordinates to discuss the audit objectives, audit scope (more detailed), audit schedule, audit process and methodology, audit team details, escalation routes on both sides, turn-around-time for provision of information or records, and initial data requirement is discussed and agreed. Usually, a presentation is made by the internal auditor covering all these aspects and inputs, from the auditees are invited to the same.

Exchange of views and clarifications from both sides enables better understanding of the expectations from each side and helps in avoiding debate about scope of audit and process to be followed for finalisation of the internal audit report later. Further, it helps in improving the perception of the internal audit activity since auditees can understand it better.

Process Walkthrough(s)

Process walkthroughs are step-by-step demonstrations or explanations of a process or task conducted by the process or task owner in the presence of the internal auditor. Internal auditor can use process walkthroughs to understand the process flow and identify the design of the internal controls using one or two examples chosen by the auditee for such demonstration. It helps the internal auditor in understanding how the auditees are conducting their day-to-day work, in relation to the internal audit engagement objectives, and identify the key controls or stage gates which ensure that the desired output of the process is achieved by the organisation.

While in case of mature control environments, the flow charts explaining the flow of information and key stage-gates / key controls of the process are already documented, yet there are many organisations where such documentation may not be available to a level which is detailed enough, or self-explanatory to meet the purposes of an internal auditor. In such cases, the internal auditors need to draw their own flow charts to obtain a complete understanding of the process. A flow chart provides a visual sequence of the steps in a process, illustrates the relationship between parts, and identifies what the process does or should do. Flowcharts can be created in a variety of ways by the internal auditors, from informal pencil drawings on scraps of paper to technically sophisticated computer graphics. Creation of flow charts by internal auditor based on process walkthroughs has following advantages:

- In the process of creating the flowchart, internal auditor can discover weakness in controls such as weak responsibility/accountability definitions, supervision by the wrong level of the organization, failure to segregate functions to avoid conflict of interest, and so on.
- A flowchart can provide an accurate description of process design, and later on when an internal auditor finds some exceptions to the process, it is easy to understand the risk or potential impact of that observation on the outcome of the process.

While making the flow charts, an internal auditor may need to keep revising the flow charts created by him/her as and when the understanding of the process interlocks becomes more and more clear. Reading of documented process documents, policies, authority matrix etc. are important before finalising process flow chart after process walkthroughs, since sometimes and actual process being explained by auditee and the requirement of approved policies may be different.

After a process walkthrough, internal auditor should be able to identify the process design gaps or risks which remain unaddressed if the same process continues in future also. Note that the risks to be identified should be in line with the audit objectives as well as process objectives. The quality of internal audit outcome is directly dependent on the quality of probing questions made by internal auditor during process walkthrough stage, and breadth of key risks identified.

Example:

While conducting an audit engagement of a payroll process, the client or management may have defined the audit objective to check the accuracy of payroll disbursed in the audit coverage period.

However, while conducting the process walkthroughs, an internal auditor is required to cover the entire process of managing the employee masters, payroll masters, payment controls in the bank accounts used for payroll related payments, the process for modifying these masters, and the tools used etc. and identify the key process controls mitigating the risk of erroneous or fraudulent payroll payments as well as regulatory and compliance risks applicable to the organisation. Thus, internal auditor must understand the entire process of arriving at the payroll calculations, payment controls and also include the related regulatory aspects in his walkthrough discussions to arrive the risks to be covered during the audit fieldwork stage and not limit the discussion on the payroll calculation sheets only.

After the process walkthroughs are completed, the process design gaps as well as additional data requirements are suitably discussed by the internal auditor at appropriate levels with process owners.

As per SIA 310 (Planning the Internal Audit Assignment), Section 3.3 states that a comprehensive knowledge of the Auditable Unit under review, its business and operating environment, shall be undertaken to determine the nature of audit procedures and tests to be conducted. As part of the planning process, a discussion with management and process owners shall be undertaken to understand the intricacies of each process considered for review.

Internal Audit Fieldwork

The internal audit fieldwork concentrates on determining whether the controls identified during the process walkthroughs are operating effectively and, in the manner described by the auditee. This stage concludes with a list of draft findings from which the auditor may prepare a draft audit report after a series of discussions with the auditees.

After gaining an understanding upon the process and identifying the risks to be audited in line with the audit objectives, the internal auditor needs to identify the data reports and relevant records of documents which need to be reviewed by him/her. Validation of the data reports received by internal auditors is a key step before the start of data analysis. It is also essential to analyze the outliers, if any, and understand the same through discussions and email confirmations with auditees, before proceeding with further checks. Sometimes, a discussion on the outliers in data reports may also result in finding out certain aspects of process which may have been missed to be discussed during process walkthroughs. Also, where possible a check on the integrity of data reports should also be made by reconciling the data received from related reports received from other authentic sources of information. In cases where the auditee claims some information or document is not available at all, the internal auditor must create a documented communication with the auditee to keep the same as evidence.

Documents and reports received are reviewed and corroborated with the explanations received, keeping in view the audit objectives. Various techniques such as document review, observation of process execution, interviews, data analysis, reconciliations, and benchmarking etc. are used by internal auditors to complete various checks planned by working out a detailed work program.

The work program shall have the details of risks identified, related controls understood, audit steps conducted to review the actual existence of such controls, and the results of the same. A work program is not a static document, but a work-in-progress or dynamic document which is updated by the internal auditor every day as the audit field work progresses. The work program also needs to clearly identify the sampling process and the rationale behind the same. While in some cases focused sampling after data analysis is effective, in other cases a stratified sampling approach is advisable.

SIA 310 (Planning the Internal Audit Assignment) Section 3.4 states that a risk-based planning exercise shall form the basis of the Internal Audit Assignment Plan. The Internal Auditor shall undertake an independent risk assessment exercise to prioritise and focus audit work on high-risk areas and processes, with due attention given to matters of importance, complexity and sensitivity.

Now we will discuss the specific aspects of the internal audit of various processes in detail keeping in view the discussion made so far.

INTERNAL AUDIT OF PURCHASING ACTIVITY

The term “purchase” refers to the act of acquiring or obtaining something by paying money or exchanging something of value for it. In other words, it is a transaction where a person or organization buys goods or

services in exchange for payment. The term "purchase" can be used in various contexts, such as personal shopping, business procurement, or even in the acquisition of assets or property. In the context of internal audits, we will use the term purchase with respect to business related procurement.

The purpose of a purchasing or procurement process in a company is to acquire the goods and services necessary for the business to operate efficiently and effectively. The term "procurement" refers to the process of identifying the need for goods and services, selecting vendors or suppliers, negotiating contracts, purchasing the items, and ensuring that they are delivered in a timely and cost-effective manner.

The procurement process serves several purposes in a company, including:

1. ***Ensuring the availability of goods and services****:* The procurement process ensures that the company has access to the goods and services it needs to operate, such as raw materials, equipment, or office supplies.
2. ***Maximizing value for money****:* The procurement process aims to obtain the required goods and services at the best possible price, quality, and delivery time. This can help the company to reduce costs and increase efficiency.
3. ***Managing risks****:* The procurement process can help the company to manage risks associated with supply chain disruptions, quality issues, or regulatory compliance.
4. ***Building relationships with suppliers****:* The procurement process can help the company to build and maintain good relationships with suppliers, which can lead to better pricing, more reliable delivery, and improved quality of goods and services.

Thus, the objective or purpose of conducting an internal audit of Procurement process is to provide assurance to the audit committee or board, that the procurement process is being executed effectively and efficiently, and to identify areas for improvement. Some of the specific objectives of a procurement audit may include are:

1. ***Ensuring compliance with policies and regulations****:* Internal audit can determine if the procurement process is following established policies and procedures, as well as regulatory requirements such as local laws and regulations, international trade regulations, and other legal requirements.
2. ***Evaluating the effectiveness of the procurement process****:* Internal audit can assess the effectiveness of the procurement process in meeting its goals, such as obtaining goods and services at the best possible price, quality, and delivery time.
3. ***Identifying opportunities for cost savings****:* Internal audit can identify areas where the procurement process can be improved to achieve cost savings or cost avoidance, such as reducing waste, optimizing inventory levels, or negotiating better prices with suppliers.
4. ***Assessing supplier performance:*** Internal audit can evaluate the performance of suppliers to determine if they are meeting contract requirements, delivering goods and services on time, and meeting quality standards.
5. ***Improving risk management****:* Internal audit can identify areas of potential risk in the procurement process, such as fraud, corruption, or conflicts of interest, and recommend ways to mitigate those risks.

Considering above audit objectives, the internal auditor usually sends the audit notification on email to the respective function owners and the other interested members of senior management. Such audit notification may generally include the following contents:

- *Audit Name or Title* (for instance, Review of Procurement Process").
- *Audited Company:* This is more applicable in case the company is a conglomerate and the internal auditor is responsible for more than one company.

- *Audit Coverage Period:* As a general practice, last 12 months before the planned start of internal audit are taken as audit coverage period.
- *Audit Objective (s):* This is generally in line with the objectives already discussed previously in this chapter.
- *Audit Scope:*
    a. Procurement of raw materials, consumables and finished goods.
    b. Procurement of Services for services etc.
- Auditee Departments:
    a. Purchasing department
    b. Administration department
    c. Finance department
    d. Customer service department etc.
- Proposed Kick off meeting date / time slots.
- Auditor details (a firm's name or an internal audit department's employee)
- Proposed schedule of audit

After releasing the internal audit notification, (and before the kick-off meeting), the internal auditor usually works together with the function head to detail out the scope of audit as well as agree on the schedule of audit within a reasonable range of the schedule already approved by the audit committee.

A typical detailed scope of "Review of Procurement Process" may include the following:

1. **Reviewing the vendor selection process** in terms of following:
    - Process to define the specifications/requirement (Material or Service Requisition Process).
    - Approvals for going ahead to procure the requirement (Requisition Approvals).
    - Process to identify the vendors who are qualified to bid for the requirement (Pre-qualification process).
    - Process to define contents of Request for Proposal (RFP) / Request for Quotation (RFQ) along with the criteria to be used for their evaluation after bids are received. The criteria are defined together with RFP / RFQ to ensure that all information required for bids evaluation is asked for in the RFP / RFQ. These criteria usually include the standard terms and conditions drafted by the legal department of procuring organisation, which the bidder needs to agree and adhere to, if selected.
    - Process for evaluation of bids received based on QCDM parameters.
        – Quality (Q) – while the bidders have already passed the pre-qualification stage, and thus are supposed to meet the minimum requirements of requisition, the assessment at this stage is to rank the bidders based on the bids received, as well as the discussions that may be held with the bidders to understand their alignment to requirements.
        – Cost (C) – scores or ranking is given based on the quoted amount. While the lowest bidder is given the highest score the highest bidder gets the lowest. This also includes an evaluation of other financial terms and conditions such as payment terms or credit period, advance moneys requirement, readiness to provide security deposits or bank guarantees etc.

- Delivery (D) – delivery scores are based on the schedule or delivery of materials or service as offered by the bidders. The bidder providing the delivery earlier than others shall get the maximum scores and so on. However, it must be kept in mind that the delivery committed by the bidder should not be impractical. In such case, a discussion should be held with the bidder to ensure that the requisition is understood properly by the bidder and their delivery schedule is based on correct assumptions or not.
- Management (M) – management scores are given based on the overall strength of the organisations bidding. This includes the size of the organisation, their existing customers, financial position, and experience of working in similar conditions earlier etc. Scores in this criterion help in identifying the bidder which is a better fit for the procuring organisation.

- Process to sign the contracts or issuing the purchase order with standard legal terms and conditions agreed with the bidder.
- Process to register the vendor (Vendor Registration).

In the entire process above, a review of the *Segregation of duties*, *documentation* created by the auditee departments and adherence to defined *approval matrix* and defined *process stage gates* are critical for an internal auditor.

2. Reviewing the Procurement Process:

Depending upon the nature of procurement the organisations may decide some procurements to be done through a Purchase Order (called as PO route), and some procurements to be made without a Purchase Order (called as non-PO route).

Following scope items are generally applicable in case of procurement by PO route:

- Review adherence to Delegation of Authority (DOA) for issuance of PO.
- Reviewing 3-way match controls (Purchase order, Goods Receipt Note (GRN) and invoice booking).

  This process step involves checking whether the requirement defined in PO has been received as evidenced by GRN, and whether the supplier invoice matches with the received quantity as per GRN and price as per PO. This matching is required before any payment can be made to a vendor. While this process can be automated in an ERP environment, it may be partially automated or manual in a non-ERP environment. This checking includes the checks to ensure compliance with agreed terms and SLAs before processing the invoice and payment.
- Review PO/signed agreement terms and conditions (T&Cs).

  This is to observe if any waivers on standard T&Cs have been granted to the vendors with the exception approvals being taken. While enforcing T&Cs with vendors may not be possible, an exception route definition should exist in the policy to approve for the exceptions.
- Review the process of accounting of procurement, and related segregation of duties within the accounting function including review of accounting system controls on invoice booking and payment processing.
- Review of payment process including bank payments process and cash payments process (if any) and review of appropriateness of supporting evidence.
- Review of levy of any interest, penalty or liquidated damages as per the agreed T&Cs.
- Review of segregation of duties with respect to PO creation & approval, expense approval, receipt of goods/ services, accounting and payment processing is an integral part of a Procurement Review.

Following scope items are generally applicable in case of procurement by non-PO route:

- Review to ensure that expenses are approved as per company policy or delegation of authority.
- Review of terms agreed with the vendors.
- Review of process to ensure desired receipt of goods/services and invoice accuracy.
- Review of process to ensure compliance to agreed terms and SLAs before processing the invoice and payment, and appropriateness of supporting evidence. This also includes review of levy of any interest, penalty or liquidated damages as per the agreed terms.
- Review of accounting controls with respect to the expense booking and payment processing.
- Review process of tracking due date for payments, and reconciliation of prepaid expenses (advance moneys paid).
- Review of segregation of duties with respect to the expense approval, receipt of goods/services, accounting and payment processing.

The peculiar characteristics of non-PO route procurements are given below:

Non-PO route is generally used in case of specific services such as legal services, audit services, day to day administration expenses, and utility payments. Instead of 3-way matching, only 2-way matching is applicable in non-PO route. Since there is no PO issued, the accounting for expense is done after receipt of service or goods along with the supplier invoice only. Thus, GRN and Invoice booking is done at the same time.

Vendor selection for non-PO procurements is generally done by user departments or cross functional teams. The role of centralized procurement department is minimum, leading to non-standard practices by various functions making such procurements. Thus, the internal auditor needs to review each transaction in more detail.

Procurements through non-PO route are less controllable and thus an organisation should try to route most of the procurements through PO route as far as possible.

An internal auditor needs to consider the discussion above and identify the risks applicable to the organisation process during the process walkthrough and the audit fieldwork. While each organisation may have peculiar risks applicable to their industry processes, general risks associated with a procurement process could be as follows:

1. Vendor favouritism
2. Non-transparent vendor selection without involving all stakeholders
3. Requisition specifications tweaking to benefit a specific vendor
4. Appropriate approvals not in place before effecting the transactions
5. Segregation of duties issues across the process
6. Order is placed with different content than the approved one
7. Materials not received on time resulting in delayed deliverable to end customer
8. Supply chain over-dependence on some vendors
9. Liquidity of financial risks of vendor resulting in supply chain disruption for the organisation
10. Vendors not meeting the Quality, Health and Safety norms resulting in risks for the procuring organisation

11. Vendors not providing the quality and quantity promised, especially in Just in Time procurement scenarios
12. Payment terms and other T&Cs do not meet company's payment rule
13. Use of excess or lower accruals by finance department to "manage" the financial results or keep some amounts for "rainy days"
14. Account code is not used appropriately
15. Double / multiple payment risks especially in non-PO route payments
16. Inefficient or delayed payment settlement process leading to vendors asking for higher rates due to their working capital blockage.

The risks can be more and less depending upon each organisation and an internal auditor needs to identify and audit the same using his/her professional skills while keeping in mind the process objectives and audit objectives. Once risks are identified, the internal auditor needs to look for the process controls which enable mitigation of these risks, and if any risk is not mitigated then the same shall be reported as a process design gap. Further, internal auditor needs to audit the operating effectiveness of the process by using various techniques to check whether currently designed process is working effectively to mitigate the risks identified or not. Suitable reporting is then required to be made to the auditees, and management and the audit committee or board.

INTERNAL AUDIT OF INVENTORY MANAGEMENT

The term "Inventory" refers to the stock of goods or materials that a business or organization has on hand for sale or production. It can include finished products, raw materials, work-in-progress items, and other items that are used in the production or distribution process.

The purpose of inventory management is to ensure that a company has enough stock to meet customer demand while avoiding overstocking that can lead to waste or additional costs. Proper inventory management can help a business maintain a steady supply of products, maximize efficiency, and minimize costs.

The purpose of inventory management in an organization is to ensure that there is an optimal level of inventory always maintained. Inventory management involves tracking the inventory levels, ordering new stock, and managing the flow of goods in and out of the organization. Effective inventory management has several benefits for an organization.

First, it ensures that there is enough inventory available to meet customer demand. This helps to avoid stockouts, which can result in lost sales and dissatisfied customers. Second, inventory management can help to reduce the cost of carrying inventory. By tracking inventory levels and ordering only what is needed, organizations can minimize the amount of capital tied up in inventory and reduce the cost of holding and storing inventory. Third, inventory management can help to improve cash flow. By minimizing the amount of capital tied up in inventory, organizations can free up cash to invest in other areas of the business. In a manufacturing organisation, in addition to the objective of maintaining optimum inventory, there is also an objective to ensure no line stoppages and ensure minimum wastage in the manufacturing process.

Overall, effective inventory management is essential for organizations to ensure that they have the right products available at the right time and at the right cost, which is critical for success in today's competitive business environment.

Inventory is required to be kept by an organization for any of the following purposes:

- held for sale in the ordinary course of business; or
- in the process of production for such sale; or

- in the form of materials / supplies to be consumed in the production process or in the rendering of services.

Inventory could be related to raw materials (parts, consumables), finished goods, spare parts, defective products or parts or scrap, and goods in transit. The key costs that apply to inventory management are *inventory holding cost, inventory ordering costs, investment cost, and space management costs.*

Holding cost, also known as carrying cost, is the cost that a business incurs for holding inventory in stock over a period of time. It includes various expenses related to storing and maintaining inventory such as rent, utilities, insurance, security, labor, and opportunity cost of capital. The longer the inventory is held in stock, the higher the holding cost will be. Therefore, it is important for businesses to optimize their inventory levels to minimize their holding costs. This can be achieved by implementing efficient inventory management practices such as just-in-time (JIT) inventory systems, economic order quantity (EOQ) models, and inventory turnover analysis. By minimizing the holding cost of inventory, businesses can improve their profitability and cash flow. However, it's important to strike a balance between holding costs and the risk of stockouts, which can result in lost sales and dissatisfied customers.

Inventory ordering costs, also known as setup costs or procurement costs, are the costs associated with placing and receiving orders for inventory items. These costs include expenses such as purchase order processing, supplier communication, shipping and handling, and inspection upon delivery. The ordering cost can vary depending on the quantity of items ordered and the frequency of orders placed. For instance, if an organization places fewer but larger orders, the ordering cost per unit may be lower. However, if an organization places more frequent but smaller orders, the ordering cost per unit may be higher. To optimize their inventory ordering costs, businesses can use various strategies such as batch ordering, where they order items in larger quantities to reduce the frequency of orders and hence, the ordering cost per unit. Alternatively, businesses can use supplier-managed inventory (SMI) systems, where suppliers are responsible for monitoring inventory levels and automatically replenishing stock when needed. Overall, effective management of inventory ordering costs is important for businesses to maintain an optimal level of inventory while minimizing the associated costs.

Investment costs in relation to inventory, also known as capital costs, are the costs associated with acquiring and holding inventory. These costs include expenses such as the initial purchase price of the inventory, storage costs, and the opportunity cost of capital tied up in inventory. The opportunity cost of capital is the cost of the forgone alternatives, which is the cost of the next best opportunity that could have been pursued if the capital was not tied up in inventory. For example, if an organization invests 10,000 in inventory and earns a 10% return on investment annually, the opportunity cost of capital tied up in inventory is 1,000 per year. Investment costs can have a significant impact on the profitability and cash flow of a business. Therefore, it's important for businesses to optimize their inventory levels to minimize their investment costs. This can be achieved by implementing efficient inventory management practices such as ABC analysis, safety stock calculation, and lead time management. By optimizing their inventory investment costs, businesses can improve their profitability and cash flow. However, it's important to balance inventory investment costs with the risk of stockouts, which can result in lost sales and dissatisfied customers.

Space management costs are the expenses associated with the physical space required to store inventory. These costs include rent or mortgage payments, utilities, insurance, property taxes, and maintenance expenses. Space management costs can have a significant impact on the profitability and cash flow of a business, especially if the organization stores excessive inventory. Therefore, it's important for businesses to optimize their inventory levels to minimize their space management costs. One way to minimize space management costs is to implement efficient inventory management practices such as just-in-time (JIT) inventory systems, which emphasize smaller and more frequent deliveries of inventory, and economic order quantity (EOQ) models, which calculate the optimal order quantity to minimize total inventory costs. Another way to minimize space management costs is to optimize the use of available space by using inventory management software, labeling

and organizing inventory, and using vertical storage solutions such as pallet racks and mezzanine floors. Overall, effective management of space management costs is important for businesses to maintain an optimal level of inventory while minimizing the associated costs. By optimizing their inventory space management costs, businesses can improve their profitability and cash flow.

An understanding of various costs applicable to inventory management is essential for an internal auditor to ask effective probing questions during the process walkthrough stage and identify the pertinent risks applicable to an organization that he/she is auditing.

Thus, the audit objective of "Review of Inventory Management Process" is generally to provide and assurance to the audit committee or board on the following topics:

- Adequacy of inventory control process policies and procedures and their appropriate implementation.
- Appropriateness of roles and responsibilities, including the segregation of duties in the key processes.
- Effectiveness of physical and operational controls in place for effective inventory management.
- Completeness and accuracy of reporting or recording of all inventory transactions in the financial system and adequacy of monthly and year end reporting procedures.

While conducting process walkthroughs, an internal auditor needs to understand the entire process of inventory management by meeting all stakeholders including purchase department, stores department, manufacturing department or other departments responsible for material requisitions, and accounting and finance departments. Further below given points should be specifically focused upon during these discussions:

- inventory planning process by various stakeholders
- materials receiving process
- warehousing standards and procedures including physical controls
- process for issuing the materials for production/operations
- process for assembly of any inventory items before issuing to production / operations
- shipping process for finished goods
- cyclical and periodic physical counts, and
- financial reporting and monthly and year-end procedures.

To conduct an internal audit of inventory management process, an internal auditor must understand document flow along with the physical movement of materials and goods. Thus, a physical visit to relevant locations is indispensable. Further, a clear and unambiguous understanding regarding the relevant management information systems and the reports thereof is necessary to understand how the function heads control the entire process. These discussions need to be done with a focus to identify the process used by auditees for identifying outliers, and detection of avoidable leakages. Further, the discussions should include the questions to assess the segregation of duties in entire process as well.

Additionally, an internal auditor needs to focus on process controls to detect and deal with stock losses, management of any rejected materials (including the legal recourse available against vendors as per agreed terms), and process to manage obsolete and scrap materials including the disposal process. Scrap management and its disposal process needs to be reviewed from the point of view of theft and pilferage risks.

Further, specific focus on the aspects is also generally required with regards to process controls ensuring correct accounting of inventory in books. For instance: Capital or revenue decision, inventory items used for research and development, inter unit transfers, valuation norms, proper maintenance of items master and giving

effect to results of physical count in the books. The accounting assertions given below should be kept in mind by the internal auditor while conducting this review:

Accounting Assertions:

- Existence
- Completeness
- Accuracy
- Classification
- Cut-off
- Realizable value
- Rights
- Presentation and Disclosure

An internal auditor needs to consider the discussion above and identify the risks applicable to the organisation process during the process walkthrough and the audit fieldwork. The risks can be more or less depending upon each organisation and an internal auditor needs to identify and audit the same using his/her professional skills while keeping in mind the process objectives and audit objectives. Once risks are identified, the internal auditor needs to look for the process controls which enable mitigation of these risks, and if any risk is not mitigated then the same shall be reported as a process design gap. Further, internal auditor needs to audit the operating effectiveness of the process by using various techniques to check whether currently designed process is working effectively to mitigate the risks identified or not. Suitable reporting is then required to be made to the auditees, and management and the audit committee or board.

INTERNAL AUDIT OF PRODUCTION AND OPERATIONS

Production refers to the process of creating or manufacturing goods or services that can be sold in the market. It involves transforming raw materials, components, or other inputs into finished products or services that meet the needs of customers. The production process typically involves a series of steps, such as designing the product, sourcing raw materials or components, assembling or processing the inputs, quality control, and packaging or labelling the finished product. The main goal of production is to create goods or services that can be sold in the market and generate revenue for the business. Efficient production processes can help businesses to reduce costs, increase productivity, improve quality, and meet customer demands. There are different types of production methods used by businesses, such as mass production, batch production, job production, and continuous production, each with its own advantages and disadvantages depending on the nature of the product or service being produced and the needs of the business.

The term Operations, however, refers to the activities involved in managing and controlling the processes that create goods and services within an organization. It includes all the tasks and functions required to transform inputs such as raw materials, labour, and capital into finished products or services that can be delivered to customers.

Operations management is a critical component of any business and involves various functions such as planning, organizing, controlling, and coordinating resources to achieve the objectives of the organization. The primary goal of operations management is to optimize the efficiency and effectiveness of operations while ensuring high-quality products and services. Some of the key activities involved in operations include:

- *Capacity planning* - determining the resources needed to meet customer demand.

- *Production planning and scheduling* - planning and scheduling production processes to ensure efficient use of resources.
- *Inventory management* - managing inventory levels to ensure that there is enough stock to meet customer demand while minimizing costs.
- *Quality control* - ensuring that products or services meet the required quality standards.
- *Supply chain management* - managing the flow of goods and services from suppliers to customers.

By managing operations effectively, organizations can improve their competitiveness, increase customer satisfaction, reduce costs, and ultimately achieve their strategic objectives.

By understanding the above terms in general parlance, it comes out that a "Review of Production and Operations" in internal audit shall entail covering the production planning and scheduling, quality control, inventory management and supply chain management for an organisation. However, considering the size of some organisations the same may not be possible to cover in a single audit and thus may be split into various separate audits such as Production audit, Inventory Management audit and Supply chain audit. Due to this, in this section of the lesson, we will concentrate our discussion on the production process and related controls only.

Production is a scientific process which involves transformation of raw material (input) into desired product with the help of energy, capital, manpower and machinery and is a very complex process. The key process objectives of a production process generally are:

- On time-every time,
- Zero quality issues, and
- Controlled wastages.

"On time every time" is an objective of the production process that refers to the ability to consistently deliver products or services to customers on or before the agreed-upon delivery date or time. It is a measure of reliability and consistency in meeting customer expectations and is often a critical factor in achieving customer satisfaction. It involves ensuring that all aspects of the production process are well-organized, efficient, and reliable, from raw material procurement to finished goods delivery. This includes managing the supply chain, scheduling production runs, ensuring sufficient inventory levels, and maintaining high levels of quality control. Meeting the "on time every time" objective requires a well-organized and efficient production process that can respond quickly to changes in demand or unexpected production issues. To achieve this objective, organizations need to have effective production planning and scheduling systems, robust inventory management practices, and streamlined logistics and delivery processes. By meeting the "on time every time" objective, businesses can build a reputation for reliability and trust with their customers, which can lead to increased customer loyalty, repeat business, and positive word-of-mouth recommendations.

The "zero quality issues" objective in a production process refers to the goal of achieving a production process that has no defects or errors in the finished products. It is a measure of the quality and reliability of the production process and is a critical factor in meeting customer expectations. The "zero quality issues" objective involves implementing a comprehensive quality management system that ensures that all aspects of the production process are designed, monitored, and controlled to minimize the risk of quality issues. This includes managing the supply chain to ensure that raw materials are of high quality and meet specifications, implementing robust quality control processes during production, and conducting thorough testing and inspection of finished goods. To achieve the "zero quality issues" objective, organizations need to implement a culture of continuous improvement that emphasizes the importance of quality in all aspects of the production process. This includes providing regular training and development opportunities for employees, encouraging teamwork

and collaboration, and implementing data-driven performance metrics to monitor and track progress towards the objective. By achieving the "zero quality issues" objective, businesses can build a reputation for producing high-quality products that meet customer expectations, which can lead to increased customer satisfaction, brand loyalty, and positive word-of-mouth recommendations. It can also help to reduce costs associated with quality issues such as product recalls, warranty claims, and customer returns.

The objective of "controlled wastage" in a production process is to minimize the amount of material waste generated during the manufacturing process while ensuring that the final product meets the required quality standards. It is a measure of the efficiency and sustainability of the production process. The "controlled wastage" objective involves implementing a comprehensive waste management system that aims to reduce, reuse, and recycle materials wherever possible. This includes optimizing the use of raw materials, implementing effective inventory management practices, and controlling the use of resources such as energy, water, and packaging materials. To achieve the "controlled wastage" objective, organizations need to identify and measure the amount of waste generated at each stage of the production process and implement strategies to reduce waste wherever possible. This may include reusing materials or incorporating recycled materials into the production process, implementing lean manufacturing principles to eliminate waste, and implementing best practices for managing hazardous materials. By achieving the "controlled wastage" objective, businesses can reduce costs associated with material waste, improve the sustainability of their operations, and reduce their environmental impact. It can also help to enhance the reputation of the organization as a socially responsible and environmentally conscious business.

The students may observe that all of these three objectives of a production process are intertwined with each other and also with the other sub-ordinate or feeding processes of the organization. However, while conducting an internal audit, an internal auditor cannot review all of these aspects in one go. Therefore, it is recommended to break up the entire scope into 2 to 3 separate internal audits and get approvals on the scope from the audit committee or board in accordance with the same. Further, the audit objective of a production and operation process is generally described as below:

To provide an assurance to the audit committee and board on the:

- adequacy of designing of existing control framework for production,
- process and appropriate implementation of such controls,
- appropriateness of roles and responsibilities, including the segregation of duties for key processes involved under production activity,
- optimum utilization of all the resources with minimum wastage and maximum achievement of quality of the product, and
- the procedures for ensuring accuracy of the production information in the financial system.

The risks generally covered in a production process audit are described below (this is not an exhaustive list):

i. Materials may be delivered late or may not be delivered at all, impacting the production plan.

ii. Associated departments may have fallen behind in their own production resulting in line stoppages.

iii. Risk of excessive absenteeism on the part of the workers resulting in line stoppages, wastages and discontent among other workers.

iv. The customer may insist on changing the specification or delivery date, but internal processes may not be geared up for the same.

v. Risk of machinery or power breakdown.

vi. Risk of errors in drawings or specification of the materials being procured or produced.

vii. Risk of rejections due to poor material quality.

viii. Errors in processing and inspection.

ix. Risk of not having adequate business continuity management processes to deal with risks such as fire, earthquake, natural calamities, cyberattack, IT system failure, etc.

x. Risk of labor unrest.

xi. Risk of regulatory non-compliances applicable to specific process.

xii. Risk of not meeting contractual norms with / by vendors.

An internal auditor needs to develop his interview questions for the process walkthroughs and ask probing questions to understand how things actually work. A physical visit to the production place is a must for an internal auditor to understand the situation properly. Based on the discussions in process walkthrough, an internal auditor can develop the work program and proceed with the audit.

INTERNAL AUDIT OF FINANCE AND ACCOUNTS

The term "Finance" refers to the management and allocation of money, assets, investments, and liabilities. It involves management of various financial systems, such as banking, credit, investments, and the distribution of resources. Finance encompasses a broad range of activities, including budgeting, financial planning, investing, and the evaluation of financial decisions with an objective of optimizing the allocation of resources and achieving financial goals. Thus, finance is a broad term encompassing a wide range of activities.

In the context of accounting and finance, accounts refer to the systematic record-keeping of financial transactions within an organization. These transactions are typically categorized and recorded in various accounts, such as revenue accounts, expense accounts, asset accounts, liability accounts, and equity accounts. The purpose of maintaining accounts is to track and summarize the financial activities of a business.

The term "Finance & Accounts" typically refers to a functional area or department within an organization that handles financial management, accounting, and related activities. It encompasses a range of responsibilities related to financial planning, analysis, reporting, and control. The key objectives of the Finance & Accounts department in a company typically revolve around ensuring effective financial management and supporting the overall financial health of the organization.

Some common objectives of a Finance & Accounts department include:

1. ***Financial Planning and Analysis:*** The Finance & Accounts department is responsible for developing financial plans, forecasts, and budgets for the company. This involves analyzing past performance, projecting future financial trends, and setting financial goals and targets.

2. ***Financial Reporting****:* The Finance & Accounts department prepares and presents accurate and timely financial reports to internal and external stakeholders. These reports include financial statements, such as income statements, balance sheets, and cash flow statements, which provide a comprehensive overview of the company's financial position.

3. ***Financial Control and Risk Management****:* The Finance & Accounts department establishes and maintains internal controls to safeguard the company's assets, ensure compliance with financial regulations, and mitigate financial risks.

4. ***Cash Management****:* Managing cash flow is a critical objective for the Finance & Accounts department. It involves optimizing the inflow and outflow of cash to ensure the company has sufficient liquidity

to meet its operational and financial obligations. This includes monitoring cash balances, managing receivables and payables, and optimizing working capital.

5. ***Capital Budgeting and Investment Analysis****:* The Finance & Accounts department evaluates investment opportunities and capital expenditure projects to determine their financial viability and potential return on investment. This involves analyzing the costs, benefits, and risks associated with various investment options and making informed investment decisions.
6. ***Financial Strategy and Decision Support:*** The Finance & Accounts department provides financial insights and analysis to support strategic decision-making within the organization. This may include evaluating new business initiatives, conducting financial feasibility studies, assessing the financial impact of potential strategies, and providing financial recommendations to senior management.
7. ***Treasury Management****:* The finance department manages the company's treasury function, which involves overseeing cash and liquidity management, optimizing debt and equity financing, managing foreign exchange risk, and maintaining relationships with banks and financial institutions.
8. ***Compliance and Regulatory Requirements****:* The finance department ensures compliance with financial regulations, accounting standards, and tax laws. This includes preparing financial statements in accordance with applicable accounting principles, filing regulatory reports, and coordinating external audits.

These objectives can vary depending on the specific industry, size, and nature of the company. The finance department works closely with other departments to support their financial needs and contribute to the overall success of the organization.

It is obvious that while conducting an internal audit, an internal auditor cannot review all these aspects in one go. Therefore, it is recommended to break up the entire scope into separate internal audits and take approvals on the scope from the audit committee or board in accordance with the same.

While conducting an internal audit of the financial reporting controls, below aspects need to be focused upon:

- **Accounting Policies:** Whether the organization being audited is having an accounting manual documenting the accounting policies to be followed. In many cases the accounting policies are documented in the annual reports also as part of the disclosure notes to accounts. A study of these policies is required before conducting process walkthroughs of accounting procedures and identification of relevant controls to be audited.
- **Closing Checklist:** Internal auditor should obtain an understanding of monthly, quarterly, and annual financial closing procedures and assess whether they are clearly defined, communicated, and implemented properly. Closing checklists play a crucial role in a financial closing process. A closing checklist in a financial closing process is a tool or document that outlines the necessary tasks and steps to be completed to close the financial books and finalize the accounting period. It serves as a guide to ensure that all critical activities are addressed and that the financial statements are accurate and complete. The specific items included in a closing checklist may vary depending on the company, industry, and the software used for accounting, but here are some common elements:

    a. ***Reconciliation of Accounts****:* Perform reconciliations for bank accounts, intercompany accounts, accounts receivable, accounts payable, inventory, and other relevant accounts to ensure that balances are accurate, and discrepancies are resolved.

    b. ***Revenue Recognition and Cut-off:*** Review transactions and ensure that revenue is appropriately recognized, cut-off dates are observed, and any required adjustments are made.

    c. ***Accruals and Deferrals:*** Assess and record accruals and deferrals, such as accrued expenses,

prepaid expenses, accrued revenue, and deferred revenue, to match revenue and expenses to the correct accounting period.

d. ***Fixed Assets:*** Verify the accuracy of fixed asset records, review depreciation calculations, and reconcile asset registers with the general ledger.

e. ***General Ledger Review****:* Review the general ledger for accuracy, completeness, and proper classification of transactions. Address any misclassifications, coding errors, or other issues.

f. ***Expense Analysis****:* Analyze expenses to identify any unusual or significant items, review expense accounts for accuracy, and ensure appropriate categorization.

g. ***Journal Entries****:* Prepare and post necessary adjusting journal entries to rectify errors, account for accruals, deferrals, and other adjustments required for the period-end closing.

h. ***Financial Statement Preparation****:* Compile and prepare financial statements, including the income statement, balance sheet, and cash flow statement, in accordance with applicable accounting standards and organizational policies.

i. ***Disclosures and Footnotes****:* Review and update financial statement disclosures and footnotes to ensure compliance with regulatory requirements and provide relevant and accurate information.

j. ***Compliance and Regulatory Requirements****:* Ensure compliance with tax laws, financial reporting standards, and other regulatory obligations specific to the industry or jurisdiction.

k. ***Review and Approval****:* Obtain appropriate approvals and review the closing process with management, ensuring that all necessary sign offs are obtained.

By following a closing checklist, companies can maintain control over the financial closing process, enhance accuracy and completeness, and facilitate a smooth transition to the next accounting period. The checklist serves as a reference to ensure that all necessary tasks are completed in a timely and efficient manner. It also serves as evidence of adequate internal controls over financial reporting.

- **IT General Controls**: Although an audit of Information Technology General Controls (ITGC) is a separate audit scope, an internal auditor should review the following as a minimum while conducting an internal audit of Finance & Accounts process:

  a. ***Segregation of Duties****:* Assess whether appropriate segregation of duties exists within the financial reporting process, ensuring that critical tasks, such as initiation, authorization, recording, and reconciliation, are appropriately segregated to prevent fraud or errors. Further, conflicting access rights should not be provided. For instance, AP module and AR module access should not be available to one individual. Similarly, access to general ledger module should be provided only to very few people, and so on.

  b. ***User Access Management****:* Evaluate the adequacy of controls around periodic access reviews to ensure that authorized individuals have appropriate access and unauthorized access is prevented. For instance, separated employees' access should be removed in a timely manner. Further, employee access should be modified if there is any change in their roles and responsibilities.

- **Manual Journal Entries:** Manual journal entries are accounting entries that are recorded manually in the general ledger or accounting system to adjust or correct the financial records. Unlike automated or system-generated entries, manual journal entries are typically made outside of the regular transactional processes. They are used to reflect accounting transactions or events that cannot be captured through the normal course of business operations or to correct errors. Thus, the number of

manual journal entries passed in the accounting system should be limited and not high. Here are some common situations where manual journal entries may be necessary:

a. ***Adjusting Entries**:* Manual journal entries are made to adjust accounts at the end of an accounting period to ensure accurate financial reporting. These entries account for items such as accruals, deferrals, depreciation, prepayments, and estimates.

b. ***Correction of Errors**:* Manual journal entries are used to correct errors discovered in the financial records. This can include misclassifications, posting errors, transposition errors, or any other mistakes that require rectification.

c. ***Reversing Entries**:* Reversing entries are often created at the beginning of an accounting period to reverse the impact of certain accruals or deferrals recorded in the previous period. They simplify the subsequent accounting process and ensure that appropriate adjustments are made.

d. ***Intercompany Transactions**:* Manual journal entries may be used to record intercompany transactions between entities within the same organization. These entries facilitate the elimination of intercompany balances and ensure accurate consolidation of financial statements.

e. ***Reclassifications:*** Manual journal entries are made to reclassify transactions between different accounts or categories within the general ledger. This is done to correct misclassifications or to ensure that financial information is presented in the appropriate financial statement line items.

f. ***Reserves and Provisions**:* Manual journal entries may be used to establish or adjust reserves and provisions for contingencies, bad debts, warranties, or other uncertain liabilities.

g. ***Foreign Currency Adjustments**:* If a company operates in multiple currencies, manual journal entries may be necessary to record currency conversions, adjust foreign currency balances, or account for foreign exchange gains or losses.

It is important to note that while manual journal entries are sometimes required, organizations should strive to minimize their use and rely on automated processes and internal controls wherever possible to enhance accuracy and efficiency in financial reporting. Proper documentation and review procedures should be in place to ensure that manual journal entries are authorized, supported by appropriate documentation, and subjected to appropriate review and approval processes.

- **Post-Close Entries:** Post-close entries, also known as post-closing entries or year-end entries, are entries made after the closing of the accounting period. These entries are made to prepare the general ledger for the subsequent accounting period and to reset the temporary accounts to zero balances. Post-close entries are necessary to ensure that the beginning balances of the new accounting period are accurate and reflect only the transactions and balances relevant to that period. The main purpose of post-close entries is to separate the income and expense accounts from the retained earnings account, so that the income statement accounts start with zero balances in the new period and only the net income or loss from the previous period is carried forward to the retained earnings account. Post-close entries typically include the following:

  a. ***Closing entries:*** These entries transfer the balances of the temporary income and expense accounts to the retained earnings or owner's equity account.

  b. ***Dividend entries:*** If applicable, entries are made to record the declaration and payment of dividends to shareholders or owners.

  c. ***Opening entries:*** These entries establish the beginning balances for the income statement and balance sheet accounts for the new accounting period.

Post-close entries are usually made once a year, at the end of the fiscal year, to prepare for the next accounting period. They are part of the closing process and ensure the accurate presentation of financial information for the new period.

The internal auditor needs to examine the completeness, accuracy and compliance with accounting standards. Each such entry must be backed up by proper documentation as well as approval flow, and the entries should be made following the policy consistent with the prior periods. This involves assessing whether similar transactions and events have been consistently accounted for and whether there have been any significant changes in accounting policies or estimates affecting the post-close entries.

- **Management Reporting and Statutory Reporting:** It is important to reconcile the management reporting results with statutory reporting results as part of a finance and accounts audit. The reconciliation ensures consistency and accuracy between the financial information presented for management purposes and the financial statements prepared for statutory reporting and compliance purposes. There can be several reasons for differences between management reporting results and statutory reporting results. Management reporting may use different accounting standards or policies compared to statutory reporting. Differences in the recognition, measurement, and presentation of financial transactions and events under various accounting frameworks can lead to variations in reported results. Similarly, Management reporting often involves certain adjustments and reclassifications that are not required for statutory reporting purposes. These may include non-recurring items, non-operating income or expenses, or management's discretionary adjustments to reflect a particular view of the company's performance. These adjustments are typically made to provide relevant information for decision-making but may not be recognized in the statutory financial statements.

  It is important for organizations to have clear and consistent processes for reconciling and addressing differences between management reporting and statutory reporting. Regular communication and coordination between the finance and accounting teams responsible for both sets of reporting can help minimize discrepancies and ensure accurate and reliable financial information.

- **Other Items:** Further, a financial reporting audit may cover off-balance sheet items, budgetary and forecasting controls as well. Note that cash management, treasury operations, financial planning and analysis etc. are separate processes and an internal auditor may conduct process walkthroughs to understand the underlying controls and review the adequacy and effectiveness of same from time to time. Generally, these processes are covered as separate audits and not as part of Finance & Accounts internal audit.

INTERNAL AUDIT OF HUMAN RESOURCES

Human resources (HR) refer to the department within an organization that is responsible for managing the human capital and workforce. It encompasses the practices, policies, and processes related to the recruitment, selection, training, development, compensation, retention, and overall management of employees.

Key areas and responsibilities within human resources include:

1. ***Recruitment and Selection****:* HR is involved in sourcing and selecting qualified candidates for job vacancies within the organization. This includes creating job descriptions, advertising job openings, conducting interviews, and making hiring decisions.
2. ***Employee Onboarding and Orientation****:* HR oversees the process of integrating new employees into the organization. This includes conducting orientation programs, providing necessary training, and ensuring a smooth transition into the workplace.

3. ***Performance Management****:* HR plays a role in establishing performance expectations, setting goals, and implementing performance appraisal systems. They provide guidance and support to managers in conducting performance evaluations and addressing performance issues.

4. ***Training and Development****:* HR is responsible for identifying training needs, designing and delivering training programs, and facilitating the development of employees' skills and competencies. This can include both technical training and professional development initiatives.

5. ***Compensation and Benefits****:* HR manages the organization's compensation and benefits programs, including salary administration, incentives, bonuses, employee benefits, and retirement plans. They ensure compliance with relevant labor laws and market competitiveness.

6. ***Employee Relations****:* HR handles employee relations matters and works to maintain a positive work environment. They address employee concerns, manage conflicts, and foster effective communication between employees and management.

7. ***Employee Engagement and Retention****:* HR focuses on enhancing employee engagement, job satisfaction, and retention. This involves implementing employee recognition programs, conducting employee surveys, and developing initiatives to promote a positive and inclusive workplace culture.

8. ***Regulatory Compliance****:* HR ensures compliance with employment laws and regulations, including equal employment opportunity, labor standards, workplace safety, and privacy laws. They stay updated on legal changes and provide guidance to the organization to maintain compliance.

A typical internal audit of Human Resource Management related processes shall thus include a review of following topics:

a. ***Hire to Retire process***: The "hire to retire" process, also known as "end-to-end employee lifecycle management," refers to the comprehensive process of managing an employee's journey within an organization, starting from their initial recruitment, or hiring to their eventual retirement or separation from the company. It encompasses all the stages and activities associated with an employee's tenure within the organization.

   In the hiring process**,** several aspects need to be checked to ensure effective and successful recruitment. Here are some key aspects to consider when evaluating the hiring process:

   a. *Job Requirements and Description:* Review the job requirements and description to ensure they are accurate, clear, and aligned with the organization's needs. Verify that the qualifications, skills, and experience mentioned are essential for the role. Checking of manpower budgeting process is an important part of this process.

   b. *Sourcing Channels:* Assess the effectiveness of sourcing channels used to attract candidates. Consider the utilization of job boards, social media platforms, employee referrals, and professional networks. Evaluate the reach, quality, and diversity of candidates obtained through each channel.

   c. *Screening and Selection Criteria:* Evaluate the screening and selection criteria used to shortlist candidates. Ensure that the criteria are objective, relevant, and fair. Assess if the screening methods, such as resume screening and initial interviews, effectively assess candidates' suitability for the role.

   d. *Interview Process:* Evaluate the interview process to determine its effectiveness in assessing candidates' qualifications and fit for the organization. Check if structured interviews, behavioral questions, and skills assessments are used appropriately. Assess the consistency of the interview process across candidates.

e. *Candidate Experience:* Assess the candidate's experience throughout the hiring process. Consider factors such as clear communication, prompt responses, respectful treatment, and a well-organized interview process. Evaluate if the organization provides a positive and professional impression to candidates.

f. *Candidate Evaluation and Selection:* Review the methods used to evaluate and compare candidates. Assess if the evaluation process is consistent and objective. Verify that decisions are based on relevant criteria and align with the organization's needs.

g. *Compliance:* Ensure compliance with relevant employment laws and regulations. Check if the hiring process adheres to equal employment opportunity guidelines, non-discrimination practices, and any other applicable legal requirements. This includes checking compliance with contracts with Registered Trade Unions etc.

h. *Background and Reference Checks:* Assess if background checks and reference checks are conducted appropriately and consistently. Verify that the information obtained from these checks is used to make informed hiring decisions.

i. *Timeliness and Efficiency:* Evaluate the timeliness and efficiency of the hiring process. Check if there are unnecessary delays, bottlenecks, or inefficiencies that may result in losing qualified candidates.

j. *Feedback:* Lastly, consider whether there is a mechanism in place to gather feedback, track hiring metrics, and continuously improve the hiring process. Assess if lessons learned from previous hires are incorporated into process enhancements.

When conducting *an internal audit of the separation process* within an organization, several aspects should be checked to ensure compliance, efficiency, and effectiveness. Here are some key aspects to consider:

a. *Policy and Procedures:* Review the organization's separation policies and procedures to ensure they are well-defined, documented, and up to date. Verify that the policies address various types of separations, such as resignations, retirements, terminations, and layoffs.

b. *Compliance with Employment Laws:* Ensure that the separation process complies with applicable employment laws and regulations. Check if all legal requirements, such as notice periods, severance pay, and salary payments, are followed correctly.

c. *Documentation and Recordkeeping:* Evaluate documentation related to separations. Check if employee separation files are maintained accurately and contain all the necessary documentation, including resignation letters, termination notices, exit interview reports, and relevant legal forms.

d. *Exit Interviews:* Assess the effectiveness and consistency of the exit interview process. Review the questions asked during exit interviews to ensure they cover relevant topics, such as reasons for separation, feedback on the organization, and suggestions for improvement.

e. *Benefits and Entitlements:* Verify that employees who are separating receive their entitled benefits and compensations in accordance with company policies and legal requirements. This includes benefits such as unused vacation or sick leave, retirement plans, health insurance, and any other applicable benefits.

f. *Access Control and Data Security:* Ensure that appropriate access controls and data security measures are in place to safeguard confidential information during the separation process. Verify that employee access to systems, databases, and physical premises is promptly revoked or adjusted according to the separation status.

g. *Return of Company Property:* Evaluate the process for the return of company property, such as laptops, mobile devices, access cards, and other assets. Check if there are clear guidelines and procedures in place to ensure the timely and complete return of company property.

h. *Knowledge Transfer and Succession Planning:* Assess if the separation process includes mechanisms for knowledge transfer and succession planning. Determine if departing employees are required to share critical information and provide assistance in transitioning their responsibilities to other team members.

i. *Communication and Documentation to Relevant Stakeholders:* Review the communication process and documentation provided to relevant stakeholders, such as HR, payroll, IT, and managers. Check if clear and timely communication is maintained to ensure a smooth separation process.

j. *Process Efficiency and Continuous Improvement:* Evaluate the efficiency of the separation process, including timelines, workflow, and coordination between departments involved. Identify opportunities for process improvements and assess if feedback from previous separations is considered to enhance the process.

By assessing these aspects, an internal auditor can help identify any gaps or areas for improvement in the separation process. It protects the organization's assets and sensitive information and promotes a positive experience for both separating employees and the organization as a whole.

Payroll refers to the process of calculating and disbursing payments to employees for their work, including wages, salaries, bonuses, and deductions. It is an essential function within an organization's human resources and finance departments. Payroll involves managing and processing financial records related to employee compensation, taxes, benefits, and other deductions. The primary purpose of payroll is to ensure accurate and timely payment to employees in compliance with employment agreements, labor laws, and tax regulations. The payroll process typically includes the following key steps:

a. *Time / Attendance Tracking:* Payroll begins with tracking employees' time and/or attendance, which may be recorded through time clocks, electronic systems, or manual timesheets. This data is used to calculate the hours worked and determine employee earnings.

b. *Gross Salary Calculation:* Salary is calculated based on the employee's regular salary, taking into account factors such as overtime, shift differentials, and bonuses etc. Other elements, such as commissions or performance-based incentives, may also contribute to the salary calculation.

c. *Deductions:* Various deductions are subtracted from the gross salary to determine the net pay or take-home pay. These deductions may include income taxes, social security contributions such as provident fund, insurance premiums, and other voluntary or mandatory deductions.

d. *Tax Compliance:* Payroll departments ensure compliance with tax regulations by accurately calculating and deducting the appropriate amount of taxes from employee earnings. They also provide the necessary documentation, such as Form 16, to employees and government agencies.

e. *Funds Administration:* Payroll may be responsible for administering employee funds, such as Provident Fund Trusts, Benevolent Funds etc. These aspects much be reviewed by the internal auditor at length in compliance with the relevant regulations and bye laws.

f. *Payroll Processing:* Once all calculations and deductions are made, payroll data is processed to generate individual employee paychecks or direct deposits. Payroll departments maintain accurate records of employee earnings, deductions, and tax information. They also generate reports for internal and external purposes, such as financial statements, tax filings, and regulatory compliance.

g. *Compliance and Audit:* Payroll processes are subject to various laws and regulations, including labor laws, tax laws, and employment regulations.

Timeliness and transparency of the payroll process are key to employee satisfaction. An internal auditor must review the process from these aspects as well. Further, *Employee Master management, Confidentiality of information, Variable pay or bonus calculations etc.* are also very important aspects to be audited by an internal auditor.

INTERNAL AUDIT OF SALES FUNCTIONS

In sales, every day is a new opportunity to contact leads, close deals, and move closer to your target. However, it's also important to step back regularly and conduct sales audits to ensure that the team is performing at a high level that meets or exceeds expectations.

A sales audit also referred to as a sales process audit is a detailed analysis of a company's sales process. This entails reviewing everything from staff, software, to strategy. Audits identify gaps and opportunities for your sales team to improve on.

The following areas need to be looked upon:

1. **Auditing Sales skills of the staff:**

   - Assessing verbal and communicative skills (how politely, clearly and effectively salespeople speak with prospects and customers);
   - Assessing problem-solving skills (how quickly and deeply salespeople can grasp a customer's problem and deliver appropriate solution);
   - Assessing planning and organizational skills (how effectively salespeople spend their working time in a long- and short-term range);
   - Assessing knowledge of industry and market (how well salespeople understand the latest trends, current market and industry situation, competition, etc);
   - Assessing knowledge of the products and services being sold (how well the salespersons know the products or services they sell – their features, benefits, purposes, technologies used, etc);
   - Assessing knowledge of current promotional and sales offers (how well the salesperson knows currently available arsenal of exclusive propositions and promotional sales offers);
   - Assessing knowledge of the target prospects and customers (how well salesmen understand their customers and know their target audience);
   - Assessing knowledge of the existing long-term customers and their respected contribution into the company's success;
   - Assessing knowledge of the company's policies, ideology and methods applied to sell goods or services.

2. **Auditing Sales documents:**

   - All the documents involved into your Sales process (whether electronic or paper documents) should be accurately composed, filled with sufficient information, properly filed and used, and then archived. Also this refers to a way of how well the sales data is handled in the company;

     The term "well" in this section means not only common understanding of a document accuracy, but also compliance with accepted corporate/industrial procedures for managing Sales docs.

- Assessing how well the sales prospects are registered and qualified by salespeople (there needs to be a special form and procedure for registering new prospects);
- Assessing how well the existing customers are registered and qualified (their personal/corporate details and all other customer relations matters should be properly inputted into CRM software, or recorded in its paper-based analogue);
- Assessing how well the following documents are composed and registered:
    - Presales docs (Inquiries, Quotations, etc);
    - Sales Orders;
    - Outline agreements (Contracts on Quantity, Maintenance, Scheduling, etc);
    - Complaints;
- Assessing how well the Shipping data is stored, maintained and analyzed;
- Assessing how well the Billing data is stored, maintained and analyzed;
- Assessing how well the current contracts and credits are maintained and serviced.

3. Auditing Sales approaches:

- Assessing the Sales policies, procedures, methods and statistics on:
    - Customer Retention;
    - Customer Follow-Ups;
    - Customer Defections;
    - Customer Satisfaction and Dissatisfaction;
    - Efficiency of Customer Claims Addressing;
- Assessing policies and strategies.

INTERNAL AUDIT OF MARKETING FUNCTIONS

An Internal audit of marketing activities involves a comprehensive examination and analysis of marketing activities, goals and objectives. The internal audit of marketing activities / department helps to create an image of the company's mission statement, objectives, corporate culture, profitability, efficiency etc. A marketing strategy audit is vital, as it makes sure the marketing is in line with corporate goals. Under the marketing strategy audit, the auditor evaluates performance by evaluating the marketing goals and objectives, in relation to the company mission and the strategy for the organization.

An internal auditor should look at not only internal factors such as the efficiency of the marketing department and their marketing plan, but also external factors including a company's customers, competition and overall marketplace.

The components of comprehensive and systematic marketing audit are the following:

Environmental Study: The environmental study enables to focus on customers and the competition. What are customers' demographics and buying habits? What are competitors doing? What is the overall condition of company's market?

Strategic Study: It involves the examining of current marketing plan and strategies and evaluate about how well or poorly they are performing. Are the marketing objectives set the appropriate ones for business?

Organizational Study: The organizational study is an internal look at the resources available in various department such as finances, time, production, labor, equipment and more. It also involves a look at the marketing team, revenue, effectiveness of the marketing plan, products, pricing and distribution channels etc.

Key Aspects of Internal Audit of Marketing

- Formal written Business plan
- Market analyzed
- Target market segment identified
- Company strengths, weaknesses, opportunities and potential threats have been analyzed (SWOT Analysis)
- Prospects and customers profiled (Both actual and Target)
- Customer needs and wants analyzed
- Customer purchasing "influencers" identified
- Competitive information gathered and compared
- Terms and conditions & Pricing Strategy
- Delivery and after sales service policy
- Product is properly positioned in the market
- Product life cycle analyzed
- Cost and pricing objectives established
- Unit cost(s) analyzed
- Promotional tools identified (discounts, allowances, freight, etc.)
- Specific business environment and economic risks determined
- Plan and budget established for marketing communications
- Sales Promotion Strategy scrutinized
- Advertising, public relations & Brand Building
- Customer service policies/plan established
- Periodically evaluated to meet customer needs
- Sales Plan
- Sales Management strategies and objectives
- Sales goal(s) and action plan
- Sales channel(s) and distribution methods/ pricing evaluated
- Competitive comparison matrix
- Strategy for penetrating new markets.

Internal Audit Checklist for Marketing (Control Parameters)

i. Whether the record of Sales Orders (SO) is maintained for all orders received from the customers and cross verification of the orders received vis-à-vis orders entered in the System is done.

ii. Whether the check list of customer order is maintained properly for all customers.

iii. Appropriate approval for dispatch of material to customers having over-due outstanding in excess of monetary credit limit.

iv. Whether the cancelled orders and orders not processed has been document along with the reasons thereof.

v. Time lag in receipt of order vis-à-vis actual dispatch of goods analyzed and reasons for delays identified and corrective action initiated.

vi. The monitoring of pending order.

vii. Access to set and modify the blacklisting option of customers for executing sales restricted to authorized persons as per segregation of duties.

viii. Access to generated sales invoice restricted to authorized persons.

ix. Periodic MIS for sales return prepared and analyzed and corrective action initiated.

x. Whether the analysis of Customer meets, Customer Satisfaction Surveys (CSS) are periodically initiated to develop market intelligence and obtain customer feedback on quality, delivery and pricing issues.

IT SYSTEM AUDIT

An audit of information technology is also known as an audit of info systems. It refers to an examination of controls of management within an infrastructure of information and technology. In other words, it is the study and assessment of the IT infrastructure, strategies and activities of an enterprise.

An IT audit is a comprehensive dive into an organization's IT infrastructure and policies. While enhancing cybersecurity for greater data protection tends to be the main goal of IT audits, there are plenty of other things they can accomplish, including (but not limited to):

- Ensuring regulatory compliance
- Improving network performance
- Evaluating disaster recovery plans

Areas to be covered under IT System Audit

1) System security

a. Antivirus software

b. Network firewall

c. Security policies and employee training

d. Intrusion alerts

2) Access controls

a. User account management

b. Passwords

c. Role-based access controls

3) Data backup and disaster recovery

a. Routine testing of backups

b. Document disposal

c. Disaster recovery plan

d. Recovery time objective (RTO) for key IT assets

4) Performance monitoring

a. Network performance

b. Outages

c. Systems development

d. Testing and implementation

5) Regulatory compliance

a. Licensing

b. Standards and regulations

Internal Audit Checklist for IT (Control Parameters)

1. Do firewalls exist on all Internet or Extranet connections?
2. Are firewalls used internally to separate networks of different security levels?
3. Is there a formal procedure for approving all external connections?
4. Is your firewall and router configured to conform with documented security standards?
5. Is your firewall's CPU utilization monitored at least every 15 minutes?
6. Are available security patches implemented within 30 days?
7. Are security patches tested before they are deployed to production systems?
8. Do all system changes go through a formal change control process?
9. Does your cryptographic solution conform to applicable international and national standards, as well as all legal and regulatory controls?
10. Are only crypto devices used that meet the approval standards and policies of your organization?
11. Are there documented processes and procedures in place for encryption keys?
12. Is access to keys restricted to the fewest number of custodians necessary?
13. Is a quarterly inventory audit performed to verify if any stored cardholder information exceeds your retention requirements?
14. Are all passwords on network devices and systems encrypted?
15. Is telnet or Rlogin used for remote system administration?
16. Is externally accessible account data transmitted in unencrypted format?
17. Is confidential account information transmitted via unencrypted email format?
18. Is strong cryptography and appropriate key controls in place to safeguard data during transmission?
19. Are modems connected to the internal systems or DMZ systems?
20. Is anti-virus software installed on all servers and workstations?

21. Have anti-virus signature files been updated to the latest signature file?
22. Is account information access on a need to know basis only?
23. Is firewall administration limited to only the network security administration staff?
24. Is at least one of the following methods used to authenticate all non-consumer users when accessing cardholder information: unique user name and password? token devices (i.e., Secure ID, certificates, or public key)? biometrics?
25. Are non-consumer users required to change their password every 60 days?
26. Are non-consumer user accounts locked within 6 invalid login attempts?
27. Are password protected screen savers or terminal locks used on all critical systems?
28. Are group passwords allowed on critical systems?
29. Are passwords required to contain both numeric and alphabetic characters?
30. Are individuals allowed to submit a new password that is the same as a previous password?
31. Are all internal and external dormant accounts removed?
32. Are applications run on default installations of operating systems?
33. Is more than one application running as the primary function of a server at any given time?
34. Are all unnecessary services disabled on a server?
35. Do you perform penetration testing on your network and applications at least once a year and after any significant modifications?
36. Is access to all audit trails logged on all critical systems?
37. Are actions related to encryption key management logged on all servers that utilize the keys?
38. Do logs include date and time stamp on all critical systems?
39. 4Are audit trails on all critical systems secured in a way that they cannot be tampered with?
40. Do you review audit logs at least once a week on critical systems?
41. Are audit logs retained for at least six months on all critical systems?
42. Are vulnerability assessments performed on the internal and external network on a monthly basis and after updates and/or upgrades to systems?
43. Is there a file integrity monitoring system in place to alert personnel of unauthorized modifications to critical systems?
44. Are security alerts from the intrusion detection sensor monitored 24 hours a day, 7 days a week?
45. Do you have Network IDS on perimeter related systems?
46. Are the latest intrusion detection system (IDS) signatures installed on all IDS sensors?
47. Is staff provided with adequate training on operational business and recovery plan execution responsibilities?
48. Are the disaster recovery plan (DRP) and the business contingency plan (BCP) tested annually?
49. Are security roles and responsibilities formally defined?

50. Are critical data backed up on a daily basis?
51. Are backup tapes stored in a location that does not require authorized access?
52. Are information security policies documented, kept current and disseminated to all employees, vendors, contractors and partners?
53. Is there a security awareness and training program in place?
54. Are pertinent security alerts monitored, analyzed and distributed to appropriate personnel?
55. Is a security incident response plan formally documented?
56. Are employees required to sign an agreement verifying they have read and understood the polices and procedures?
57. Is access to the data center restricted and closely monitored?
58. 7Are all paper and electronic media — e.g. computer, networking, and communications hardware, telecommunications lines, etc. — containing cardholder information located in a physically secure environment?
59. Have all discarded media been erased or destroyed using a formal procedure that ensures the complete deletion of all sensitive data?
60. Do you maintain strict control over the internal and external distribution of any paper or electronic media containing cardholder data?
61. Are visitors, including vendors, permitted to enter data centers or access sensitive systems without an escort?
62. Are visitors asked to sign out and turn in their badge or tag before leaving the building?
63. Is a visitor log retained for at least three months to retain a log of physical activity?
64. Are all media devices properly inventoried and securely stored?

CASE STUDY

A leading consumer goods industry in India, with a turnover of more than Rs.250 crores with activities spread across the country covering both the urban and rural markets, has been facing a downward trend in its sales along with rising marketing costs. Top management has been grappling with a changing consumer preference trend guided by the entry of a strong MNC competitor. Some major promoters and key marketing personnel have changed loyalties and have shifted to competition. The Board has been concerned about this disturbing trend and has been reviewing the strategies being adopted by the company to adapt to these changes and retain the earlier good performance.

Audit Committee meeting held along with this Board Meeting focussed on this important business issue. The Audit Committee members felt that although a reasonable assurance is being provided by the internal audit team on adequacy of controls, a consulting focus needs to be adopted and some suggestions on improving the marketing efforts is required from the team. If required, outside help from Company Secretaries could be taken, based on their experience in marketing area.

Methodology: The Chief Audit Executive (CAE) had been conducting marketing audits but primarily with a financial focus. He felt the need to have the knowledge expertise of an MBA —Marketing who could provide a greater insight into market performance. He, therefore, approached an internal audit organisation (Chartered Secretaries firm) who had the requisite expertise. However, he felt that the expertise should

also be built into the in-house internal audit team, so that as and when required, a reasonable internal audit project could be undertaken by the in-house team. The CAE insisted the presence of a member of the internal audit team as the co-ordinator who shall be attached to the outside team of internal auditors.

The starting point was a compilation of the sales performance data for the company which was arranged — zone wise, district-wise, distributor wise, sales-executive wise, product wise.

From secondary research — annual reports, visit to ROC, the published data on competitors was also obtained and compiled. Major variations were analysed. Salesforce composition was studied and their average age profile and experience profile in the organisation and in other organisations prior to joining the organisation, was also gathered.

The age profile of the distributor's association and their geographical spread was analysed, identifying the distances and other logistic issues. Channel management system including appointment, credit management, order management and administration was gathered and flow-charted. The earlier audit reports in this area were obtained. Market survey reports on the performance was also gathered. Channel monitoring MIS was obtained. On evaluation of all the data gathered, a detailed audit programme of dealer visits in select geographic regions, salesforce interviews, physical verifications, stock level management at the channel partners end, secondary sales analysis, analysis of visit reports, collection processes, scheme (for incentives and discounts) management was prepared.

The questionnaires for the interview were drafted and forwarded to all concerned and dates of interviews intimated. The logistics of travel and teams were arranged and communicated to all concerned. Gist of major observations are given below:

- Inadequate sales men in several regions though competitors had good market share.
- There was direct co-relation between the falling market share of the company's products in particular regions with low number of sales personnel for the same regions. There was also direct co-relation between the falling market share in particular regions and high turnover of sales personnel for the same regions.
- High turnover of field sales personnel - This was due to the falling market share and attention not being paid by company to improving communications with salesforce on a regular basis.
- Absence of proper monitoring of laid down policies by the field sales personnel. This was mainly due to improper monitoring of MIS sent by field sales personnel and absence of proper feedback on the same. This had resulted in field sales personnel getting lax and filing wrong/improper forms.
- Field sales personnel were carrying on some other part-time work rather than working full-time on company's work. This was a result of improper monitoring by Head of Marketing and decentralised Area Managers at various regions.
- Salesmen not making adequate calls - Call analysis reports were filled in more as a routine rather than accurate data being sent to the company. On studying the call reports, it was found that many of them were wrongly filled and in some of them even the totals did not tally from month to month.
- Salesmen fudging visit reports and travel reports. Visit reports were filed wrongly. This was brought out in surveys with dealers and retailers who gave in writing to the visiting internal audit team that there were no visits to them in last six months, though the same was being reported in the visit reports of sales personnel.

- Distributors not stocking adequate levels. Distributors were not giving accurate sales figures in their respective statements submitted to the company. Secondary sales were shown less which resulted in company having data that the distributors were saddled with stocks whereas, the actual situation was that distributors had sold the stocks and had also collected the amounts from wholesalers/ retailers. The distributors went on pressurizing the company for more incentives/discounts, informing about their stock positions being high, though the actual situation was much different.
- Inadequate coverage of the retail market - Since in many regions there were demoralized sales staff. They did not undertake their Journey Cycle Plan (routine cycle of the market) with the distributor marketing personnel regularly and left much of the same to the distributor. Many retailers were thus not serviced regularly and retailers switched to the competitor products.
- Schemes not reaching the end users - Distributors identified. Some schemes were introduced, like free oil sachets against the products, which never reached the end customers and were pilfered by the distributors who sold these sachets in cash. This was possible as the schemes were not announced properly in every region and also the main product on which the free oil sachet slogan was written could be erased out, as it was not printed but written later by sketch pens.
- Collection in cash not registered as receipts - Sales personnel made cash collections from distributors who then did not make payments to the company. On reconciliations with distributors, they produced letters from sales personnel that they had collected the money. These sales personnel had already left the company, and it was now difficult to pursue the same with sales personnel.

Recommendations: Improve penetration — introduce stronger recruitment processes, training programmes, improving policy implementation including a very strong analysis of all information received and immediate feedback for any corrective action, monitoring visit and travel reports, introducing stock levels for distributors and stockists with proper MIS to be received from the distributors / stockists and surprise verification of the MIS with actual situation, introduction of the MIS for secondary sales monitoring, scheme audits on a regular basis by internal audit, policy of not accepting cash, Palm-tops (hand held computers) for registering orders and receipts with customer acknowledgments noted in the Palm-tops. Distributors were informed that no cash transactions were permitted by the company, and they would be giving the sales personnel money at their own risk.

LESSON ROUND-UP

- In this lesson we have discussed and learn about nuances of conducting internal audit of some specific functions or processes which are usually part of most of the organisations. Such specific function includes:
  a. Internal Audit of Purchasing Activity,
  b. Internal Audit of Inventory Management,
  c. Internal Audit of Production and Operations,
  d. Internal Audit of Finance and Accounts,
  e. Internal Audit of Human Resources,
  f. Internal Audit of Sales,
  g. Internal Audit of Marketing,
  h. IT System Audit.

- The term "purchase" refers to the act of acquiring or obtaining something by paying money or exchanging something of value for it. In other words, it is a transaction where a person or organization buys goods or services in exchange for payment. The term "purchase" can be used in various contexts, such as personal shopping, business procurement, or even in the acquisition of assets or property.
- The term "Inventory" refers to the stock of goods or materials that a business or organization has on hand for sale or production. It can include finished products, raw materials, work-in-progress items, and other items that are used in the production or distribution process.
- Production refers to the process of creating or manufacturing goods or services that can be sold in the market. It involves transforming raw materials, components, or other inputs into finished products or services that meet the needs of customers. The production process typically involves a series of steps, such as designing the product, sourcing raw materials or components, assembling or processing the inputs, quality control, and packaging or labelling the finished product.
- The term "Finance" refers to the management and allocation of money, assets, investments, and liabilities. It involves management of various financial systems, such as banking, credit, investments, and the distribution of resources. Finance encompasses a broad range of activities, including budgeting, financial planning, investing, and the evaluation of financial decisions with an objective of optimizing the allocation of resources and achieving financial goals.
- Human resources (HR) refer to the department within an organization that is responsible for managing the human capital and workforce. It encompasses the practices, policies, and processes related to the recruitment, selection, training, development, compensation, retention, and overall management of employees.
- An Internal audit of marketing activities involves a comprehensive examination and analysis of marketing activities, goals and objectives. Under the marketing strategy audit, the auditor evaluates performance by evaluating the marketing goals and objectives, in relation to the company mission and the strategy for the organization.
- An audit of information technology is also known as an audit of info systems. It refers to an examination of controls of management within an infrastructure of information and technology. In other words, it is the study and assessment of the IT infrastructure, strategies and activities of an enterprise.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. One of the discounts offered by the store is in the form of payback cards where reward points are accumulated and the customer can redeem the same on subsequent purchase. The management are of the opinion that the points redeemed are to be treated as trade discount. The internal auditors are doubtful on the matter. What should be the next course of action of the internal auditor?
2. Comments on 'the cash-book showed a huge cash balance on hand consistently throughout the year".
3. Comment on the responsibilities for properly determining the quantity and value of inventories rests with the management of the entity.

4. How would an internal auditor proceed to obtain sufficient appropriate audit evidence regarding the existence and condition of inventory?
5. During the course of Internal Audit, it has been observed that No depreciation has been charged for the year in respect of spare bus purchased during the year and kept ready by the company for use as a stand-by on the ground that it was not used during the year. Comment?
6. During the course of Internal Audit, it has been observed that a sum of Rs. 1000000 is received from an insurance company in respect of claim for loss of goods in transit costing Rs. 800000. The amount is credited to the Purchases account. Comment.
7. During the course of Internal Audit, it has been observed that a loss of Rs. 200000 on account of embezzlement of cash was suffered by the company and it was debited to salary account. Comment.
8. The management of ABC Ltd., a pharmaceutical company, while valuing its finished inventory at the yearend wants to include interest on bank overdraft as an element of cost, for the reason that overdraft has been taken specifically for the purpose of financing current assets like inventory and for meeting day to day working expenses. Comment.
9. As an internal auditor, what are the major points you would see while verify / vouch the following:
    a) Loss of inventory by theft
    b) Inventory lying with sub-contractor for processing
    c) Sale of Scraps
    d) Expenditure for advertisement in newspaper.
    e) Goods sold on Approval basis.
10. As an internal auditor, what are the major points you would see while verify / vouch the following:
    a) Trade receivable
    b) Advances to suppliers
    c) Borrowing from Banks
    d) Purchase of Fixed Assets
    e) Goods lying with third party.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Special Points relating to Internal Audit in various Entities

Lesson 7

KEY CONCEPTS

■ Non-Performing Assets 'NPA' ■ Partnership Firm ■ Limited Liability Partnership 'LLP' ■ Co-operative Society

Learning Objectives

To understand:

- Who is the regulatory body of Banking Company and what are its major functions and responsibilities?
- The prudential norms of banking company and provisioning requirement in case of Non-Performing Assets 'NPA'
- Major's points / areas to be covered in case of audit of Banking Companies, Insurance Companies, Cooperative Societies, Public Sector Undertakings, Partnership, Shipping Companies, Electric Supply Company, Hotels, and Hospital etc.

Lesson Outline

Special Points relating to Internal Audit in various entities such as:

- Banking Companies
- Insurance Companies
- Cooperative Societies
- Public Sector Undertakings
- Partnership
- Shipping Companies
- Electric Supply Company
- Hotels
- Hospital
- Lesson Round-Up
- Test Yourself
- List of Further Readings

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN BANKING COMPANIES

Regulating Body

Banking Industry in India is regulated by the Reserve Bank of India (RBI) known as the Central Bank. Major functions and responsibilities of RBI are:

- Development and supervision of the banks and non-banking financial institutions
- Determining, the monetary and credit policies
- Issuance and regulation of currency
- Acting as banker to the central and state governments, commercial and other types of banks including term-lending institutions
- To regulate the activities of commercial and other banks.

Regulatory Framework

a) Banking Regulation Act, 1949;

b) Reserve Bank of India Act, 1934;

c) Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970;

d) State Bank of India Act, 1955;

e) State Bank of India (Subsidiary Banks) Act, 1959;

f) Regional Rural Banks Act, 1976;

g) Companies Act, 2013;

h) Cooperative Societies Act, 1912 or the relevant State Cooperative Societies Acts;

i) Information Technology Act, 2000;

j) Prevention of Money Laundering Act, 2002;

k) Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002;

l) Credit Information Companies Regulation Act, 2005; and

m) Payment and Settlement Systems Act, 2007.

Features of Banking Operations

- Voluminous and complex of transactions,
- Wide geographical spread of banking network,
- Diversified and large range of products and services offered,
- Extensive use of technology,
- Strict vigilance and compliance.

Form and Content of Financial Statements

- Every banking company is required to prepare a Balance Sheet and a Profit and Loss Account in the forms set out in the Third Schedule to the Act or as near thereto as the circumstances admit. Form A of

the Third Schedule to the Banking Regulation Act, 1949, contains the form of Balance Sheet and Form B contains the form of Profit and Loss Account.

- Every banking company needs to comply with the disclosure requirements under the various Accounting Standards, as notified u/s 133 of the Companies Act, 2013, in so far as they apply to banking companies.

Reporting of Fraud

Circular issued by RBI regarding liability of accounting and auditing profession, provides that "If an accounting professional, whether in the course of internal or external audit or in the process of institutional audit finds anything susceptible to be fraud or fraudulent activity or act of excess power or smell any foul play in any transaction, he should refer the matter to the regulator. Any deliberate failure on the part of the auditor should render himself liable for action".

This requirement is applicable to all scheduled commercial banks excluding Regional Rural Banks. Auditor is not expected to look into each and every transaction but to evaluate the system as a whole.

Scope of Internal Audit

- Evaluating the effectiveness of the internal control systems and monitor its application
- Review the adequacy of the risk management procedures and methodologies
- Checking the efficiency of routine operations of the bank
- Evaluate the reliability and accuracy of the financial records and reports
- Review the management information system and the efficiency of the electronic banking services
- Implementation of policies and procedures and ensure its effectiveness
- Ensure that the procedures comply with the legal and regulatory requirements
- The undertaking of fraud investigations, if required
- Ensuring the adequacy of procedures to safeguard the bank's assets
- Monitoring the bank's Non-Performing Assets (NPA) and alarming the management when required.

Conducting an Audit

1. **Understanding the Bank and its Environment:** Auditor is required to obtain understating of:
    - Bank and its Environment including Internal Control
    - Bank's Accounting Process
    - Risk Management Process.
2. **Identifying and Assessing Risk of Material Misstatements:** Auditor is required to identify and assess following risk:
    - Risks of Material Misstatements
    - Risk of Fraud including Money Laundering
    - Specific Risks
    - Risk Associated with Outsourcing of activities.

3. **Understanding the Risk Management Process:** An effective risk management system in a bank generally requires the following:

   a) **Identification, measurement & monitoring of risks**: Risks that may significantly affect the achievement of bank's goals and objectives should be identified, measured and monitored against pre-approved limits and criteria.

   b) **Control activities**: Banks must have appropriate controls to manage its risks, including, effective segregation of duties, verification and approval of transactions, setting of limits, and reporting and approval of exception.

   c) **Monitoring activities**: Independent risk management unit should be set up which regularly assess the risk management models, methodologies and assumptions used to measure and manage risk.

   d) **Reliable information systems**: Banks must have a reliable information system that provide adequate financial, operational and compliance information on a timely and consistent basis to management.

4. **Engagement Team Discussions**

   - To gain better understanding of banks and its environment, including internal control, and also to assess the potential for material misstatements of the financial statements.
   - All these discussions should be appropriately documented for future reference.
   - The discussion should be done on the susceptibility of the bank's financial statements to material misstatements.
   - These discussions are ordinarily done at the planning stage of an audit.

   a) Benefits of discussion

   - Opportunity for team members to share their insights based on their knowledge of the bank and its environment.
   - Opportunity for team members to exchange information about the bank's business risks.
   - To make an understanding amongst the team members about effect of the results of the risk assessment procedures on other aspects of the audit, including decisions about the NTE of further audit procedures.

   b) Matters to be discussed

   - Errors that may be more likely to occur;
   - Errors which have been identified in prior years;
   - Method by which fraud might be perpetrated by bank personnel or others within particular account balances and/or disclosures;
   - Audit responses to Engagement Risk, Pervasive Risks, and Specific Risks;
   - Need to maintain professional skepticism throughout the audit engagement;
   - Need to alert for information or other conditions that indicates that a material misstatement may have occurred.

5. **Establish the Overall Audit Strategy:** Establish the overall audit strategy, prior to the commencement of an audit; and involve key engagement team members and other appropriate specialists while establishing the overall audit strategy, which depends on the characteristics of the audit engagement.

6. **Develop the Audit Plan:** Develop an overall audit plan which cover details of nature, timing and extent of audit procedures planned to be performed.

7. **Execution:** Execution stage considers the following:

   - Engagement Team Discussions
   - Response to the Assessed Risks
   - Establish the Overall Audit Strategy
   - Audit Planning Memorandum
   - Determining Audit Materiality
   - Appropriateness of Going Concern.

8. **Reliance/Review of other Reports:** Auditor should consider the adverse/qualified remarks, if any, appearing in the following:

   - Previous audit reports
   - Internal inspection reports
   - RBI inspection reports
   - Concurrent/Internal audit report
   - Report on verification of security
   - Any other internal reports specially related to particular accounts.

Assessing Risk of Fraud

Assessing Risk of Fraud – As per SA 240 "The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements", the auditor's objective is to identify and assess the risks of material misstatement in the financial statements due to fraud, to obtain sufficient appropriate audit evidence on those identified misstatements and to respond appropriately. The attitude of professional skepticism should be maintained by the auditor so as to recognise the possibility of misstatements due to fraud.

The RBI has framed specific guidelines that deal with prevention of money laundering and "Know Your Customer (KYC)" norms. The RBI has from time to time issued guidelines ("Know Your Customer Guidelines – Anti Money Laundering Standards"), requiring banks to establish policies, procedures and controls to deter and to recognise and report money laundering activities.

Audit of Advances

A. Disclosure Requirements

1. Nature wise

(i) Bills purchased and discounted

(ii) Cash credits, Overdrafts and loans repayable on demand

(iii) Term Loans

2. **Security wise**
   (i) Secured by tangible assets
   (ii) Covered by Bank/Government guarantees
   (iii) Unsecured
3. **Location wise**
   1. Advances in India:
      - Priority sectors
      - Public sector
      - Banks
      - Others
   2. Advanes outside India:
      - Due from Banks
      - Due from Others:
        (a) Bills Purchased and discounted
        (b) Syndicated loans
        (c) Others

B. Classification as per prudential norms

- **Standard assets:** Assets which does not disclose any problem and does not carry more than normal risk.
- **Sub-standard assets:** Asset which has been classified as NPA for a period not exceeding 12 months.
- **Doubtful assets:** Doubtful assets Asset which has remained NPA for a period exceeding 12 months.
- **Loss assets:** Asset in respect of which loss has been identified by the bank or internal auditors or the RBI inspection, but the amount has not been written off, wholly or partly.

C. Creation of Security

- **Primary security:** Security offered by the borrower for bank finance or the one against which credit has been extended by the bank.
- **Collateral security:** It is an additional security and can be in any form i.e. tangible or intangible asset, movable or immovable asset.

Note: Security may be created by different modes like Mortgage, Pledge, Hypothecation, Lien, Assignment etc.

D. Prudential Norms

1. **Non-Performing Advances:** An Advance will be classified as NPA if:
   a) It ceases to generate income for a bank.
   b) Interest and/or instalment of principal in respect of such an advance have remain overdue or out of order for a specified period of time.

Overdue: An amount is said to be 'Overdue', if it is not paid on the due date fixed by the Bank.

Out of Order: An account should be treated as 'Out-of-order' if the outstanding balance remains continuously in excess of the sanctioned limit/drawing power. Or If there are no credits continuously for 90 days as on the balance sheet date or the credits are not enough to cover the interest debited during the same period.

2. NPA classification w.r.t. specified advances

- **Term Loans:** Interest and/or Instalment of principal has remained overdue for a period exceeding 90 days.
- **CC/OD:** The account has remained out-of-order for a period exceeding 90 days.
- **Bills Purchased & Discounted:** The Bill remains overdue & unpaid for a period exceeding 90 days.

3. Provisioning Requirements

- **Standard assets:** 0.40% (0.25% on SME/Agricultural Advances) and 1% on commercial Real Estate Loans.
- **Sub-standard assets:** 15% [Additional provision for unsecured portion is required @ 10% (5% for infrastructure advances)]
- Doubtful assets

Unsecured portion- 100%

Secured portion- 25% to 100% depending upon the period for which advance has remained doubtful.

- Upto one year – 25%
- More than one year but upto 3 years – 40%
- Above three years – 100%
- Loss assets- 100%

4. Special cases w.r.t. NPA Classification

- **Accounts regularised near Balance Sheet date:** Where it appears that an account has inherent weakness and few credits near the balance sheet tries to make it regular, the account should be classified as NPA.
- **Asset Classification borrower-wise:** All the facilities granted by bank to borrower will have to be treated as NPA and not the particular facility or part thereof.
- **Agricultural Advances/Loans:** Interest and/or Instalment of principal is overdue for two crop seasons, in case loans granted for Short Duration crops, one crop season, in case loans granted for Long Duration crops (i.e. more than 1 year).

5. Erosion in Value of Securities: In case there arise erosion in the value of security or any fraud is committed by Borrowers, banks can directly classify these accounts as Doubtful Assets or Loss Assets, irrespective of the period for which the account has remained NPA.

Erosion in the value of securities by more than 50% of the value assessed by the bank or accepted by RBI inspection team at the time of last inspection, as the case may be, would be considered as "significant", requiring the asset to be classified as doubtful straightaway and provided for adequately.

The realisable value of security as assessed by bank/approved valuers/RBI is less than 10% of the outstanding in the borrowal accounts, the existence of the security should be ignored and the asset should be classified as loss asset. In such cases the asset should either be written off or fully provided for.

6. **Agricultural Advances affected by Natural Calamities:** Where, in the wake of natural calamities, short-term agricultural loans are converted into term loans or there is rescheduling of repayment period or fresh short-term loans are sanctioned, the term loan as well as fresh short-term loan may be treated as current dues and need not be classified as NPA.

7. **Computation of Drawing Power:** All working capital limits, at all times, should be kept within both the drawing power and the sanctioned limit. Irregular accounts should be brought to the notice of the Management/Head Office regularly.

Audit Procedure

1. Aspects of Internal Control

a) Advances should be made only after evaluating creditworthiness of the borrowers and obtaining sanction from the proper authorities of the bank.

b) All the loan documents like promissory notes, letters of hypothecation, guarantee letter, etc. should be executed by the parties before advances are made.

c) While determining the loan amount to be sanctioned, sufficient margin should be kept against securities taken so as to cover any decline in the value thereof and also to comply with RBI directives.

d) Securities should be received and returned by responsible officer and should be kept in the joint custody of atleast two responsible officers.

e) Securities requiring registration should be registered in the name of the bank.

f) In the case of physical possession of goods as security, the goods should be test checked at the time of receipts. In respect of hypothecated goods not in possession of the bank, surprise checks should be made.

g) Personal inquiries should be made so as to determine market value of goods.

h) For any increase/decrease in the value of securities, drawing power should be adjusted. All the accounts should be kept within both the drawing power and the sanctioned limit at all times.

i) All irregular accounts should be brought to the notice of the H.O. regularly.

j) The operation in each advance should be reviewed at least once every year.

k) There should exist a proper system for post disbursement supervision and follow-up.

l) Classification of advances should be made as per RBI Guidelines.

m) Ensure that the funds disbursed should be utilized only for the purpose for which advances has been granted.

2. Substantive Audit Procedure

i. To verify that amounts included in balance sheet in respect of advances are outstanding at the date of the balance sheet.

ii. To verify that advances represent amount due to the bank.

iii. To ensure that outstanding amount is appropriately supported by Loan documents.

iv. To ensure that there are no unrecorded advances.

v. To verify the appropriateness of basis of valuation of advances.

vi. To ensure that the recoverability of advances is recognised in their valuation.

vii. To check that the advances are disclosed, classified and described in accordance with recognised accounting policies and relevant statutory and regulatory requirements.

viii. Ensure that appropriate provisions towards advances have been made as per the RBI norms.

A strong internal control system, including an independent and effective internal audit function, is part of sound corporate governance. Banking supervisors must be satisfied as to the effectiveness of a bank's internal audit function that policies and practices are followed and that management takes appropriate and timely corrective action in response to internal control weaknesses identified by internal auditors. An internal audit function provides vital assurance to a bank's board of directors and senior management (and bank supervisors) as to the quality of the bank's internal control system. In doing so, the function helps reduce the risk of loss and reputational damage to the bank.

The internal audit function should develop an independent and informed view of the risks faced by the bank based on their access to all bank records and data, their enquiries, and their professional competence. The internal audit function should be able to discuss their views, findings and conclusions directly with the audit committee and the board of directors, thereby helping the board to oversee senior management.

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN INSURANCE COMPANIES

An Indian insurance company is formed and registered under the Companies Act, 2013 and the aggregate holdings of equity shares by a foreign company, either by itself or through its subsidiary companies or its nominees, do not exceed twenty-six per cent of the paid-up equity capital of such Indian insurance company. The sole objects of the Indian Insurance Company shall be to carry on life insurance business or general insurance business or re-insurance business.

Verification of Premium

The premium collections are credited to a separate bank account and no withdrawals are normally permitted from that account for meeting the general expenditure. As per the policy of the insurance company, the collections are transferred to the Regional Office or Head Office. No Risk shall be assumed by the insurer without receipt of premium according to section 64VB of the Insurance Act, 1938. Verification of premium is of utmost importance to an auditor because Insurance premium is collected upon issuing policies. It is the consideration for bearing the risk by the insurance company. The auditor should apply the following procedures: –

- Before commencing verification of premium income, the auditor should look into the internal controls and compliance which are laid down for collection and recording of the premiums.
- Cover notes should be serially numbered.
- The auditor should check whether Premium Registers have been maintained chronologically, giving full particulars including GST charged as per acceptance advice on a day -to-day basis.
- The auditor should verify whether the figures of premium mentioned in the register tally with those in General Ledger.
- The auditor should verify whether instalments falling due on or before the balance sheet date, whether received or not, have been accounted for as premium income as for the year under audit.

Verification of Claims

The auditor should obtain from the divisions/branches, the information for each class of business. The auditor should determine the total number of documents to be checked giving due importance to claim provisions of higher value. The claims under policies comprise the claims paid for losses incurred, and those estimated or anticipated claims pending settlements under the policies. Settlement cost of claims includes surveyor fee, legal expenses, etc. The Claim Account is debited with all the payments including repair charges, firefighting expenses, police report fees, survey fees, amount decreed by the Courts, travel expenses, photograph charges, etc. The auditor should-

- Check whether provision has been made for all unsettled claims.
- Check whether provision has been made for only such claims for which the company is legally liable.
- Check whether provision made is normally not in excess of the amount insured.
- Check in case of co-insurance arrangements, the company has made provisions only in respect of its own share of anticipated liability.
- Check claimed paid should be duly sanctioned by the authority concerned.

Verification of Commission

The remuneration of an agent is paid by way of commission which is calculated by applying a percentage to the premium collected by him. Commission is payable to the agents for the business procured and is debited to Commission on Direct Business Account. An insurance business is solicited by insurance agents. The auditor should verify-

- Voucher disbursement entries with reference to the disbursement vouchers with copies of commission bills and commission statements.
- Check whether the vouchers are authorized by the officers- in –charge as per rules and income tax is deducted at source, as applicable.
- Test check correctness of amounts of commission allowed.
- To check whether commission outgo for the period under audit been duly accounted or not.

Verification of Operating Expenses

All the administrative expenses in an insurance company are broadly classified under 13 heads as mentioned in Schedule IV. The auditor should check-

- Expenses in excess of Rs.5 Lakhs or 1% of net premium, whichever is higher, should be shown separately; and
- Expenses not directly relating to insurance business should be shown separately for example, expenses relating to investment department, bank charges etc. Three Important Audit Points in Insurance Company Balance Sheet.

Investments

The auditor should keep in mind the following provisions related to Investments of the Insurance Act, 1938 while examining the investments-of an insurance company-

a. An insurance company can only invest in approved securities. However, it can invest otherwise than in approved securities if the following conditions are satisfied.

- Such investments should not exceed 25% of the total investments; and
- Such investments are made with the consent of board of directors.

b. An insurer should not invest in shares or debentures of insurance or Investment Company in excess of least of the following:
   - 10% of its own total assets;
   - 2% of the investee's subscribed share capital or debentures.

c. An insurer company should not invest in shares or debentures of a company other than insurance or investment company in excess of least of the following
   - 10% of its own total assets;
   - 10% of investee's subscribed share capital or debentures.

d. An insurance company cannot invest in shares and debentures of a private company.

e. The insurance companies cannot invest the funds of its policy holders outside India.

Cash and Bank Balances

- Bank reconciliation statements shall be prepared.
- The auditor should obtain confirmation of Bank Balances for all operative and inoperative accounts.
- The auditor should physically verify Term Deposit Receipts issued by bankers. Generally all cash at year end deposited as term deposit with the bank.
- The auditor should verify the deposits and withdrawals transactions at random and check whether the Account is operated by authorized persons only.
- In case of funds, in -transit, he should verify that the same are properly reflected in a reconciliation statement.

Outstanding Premium and Agents' Balance

The audit procedures, which may be followed with regards to agent's balance, are as follows:

- Verify whether agent's balances and outstanding balances in outstanding premium account have been listed, analyzed and reconciled for the purposes of audit.
- Verify whether recoveries of large outstanding have been made in post audit period.
- Verify whether there is any old outstanding debit or credit balances as at the yearend which require adjustment. A written explanation may be obtained from the management is to their nature.
- Verify that agent's balances do not include employees' balances and balances of other insurance companies.
- Verify that no credit of commission is given to agents for businesses directly procured by it.

Books, Registers & Reports

Books and Registers to be maintained by an insurer are - Register of Policies, Cashbook, Register of Claims, Ledger, and Subsidiary Records & Control Register. Reports and Returns are regulated u/s 18 of the Insurance Act 1938 where every insurer is required to furnish to the authority a certified copy of every report on the affairs of the concern. Financial Statements and Auditor's Report of Insurance Companies have been prescribed by the authority in Regulation 3 under Schedule C of IRDA.

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN CO-OPERATIVE SOCIETIES

Co-operative society is a business organisation with a special mode of doing business, by pulling together all the means of production co-operatively, elimination of middlemen and exploitation from outside forces.

Depending upon the nature and object of the society, different kinds of books and registers will be maintained, so as to disclose a proper and fair picture of financial transactions. In case of large scale co-operative organisation, different subsidiary books and registers shall be maintained and the daily summary totals will be transferred to main Cash Book. For example:

i. Daily cash sales summary register.

ii. A register of collection from debtors if credit sales are allowed by bye-laws of society.

iii. A register of recovery of loans from salaries and directly by receipts from members in case of credit society.

iv. Loan disbursement register in case of credit society.

v. Any other columnar subsidiaries depending upon the nature and functions of society.

Restrictions on share holdings-According to section 5 of the Central Act, in the case of a society where the liability of a member of the society is limited, no member of a society other than a registered society can hold such portion of the share capital of the society as would exceed a maximum of twenty percent of the total number of shares or of the value of shareholding to 1,000/-. The auditor of a co-operative society will be concerned with this provision so as to watch any breach relating to holding of shares. One should also watch whether any provision in the bye-laws of the society is not contrary to this statutory position. The State Acts may provide limits as to the shareholding, other than that provided in the Central Act.

Restrictions on loans - Section 29 of the Central Act puts restriction on loan. It states that a registered society shall not make a loan to any person other than a member. However, with the special sanction of the Registrar, a registered society may make a loan to another registered society.

The State Government may further put such restrictions as it thinks fit on the loaning powers of the society to its members or to other societies in the interest of the society concerned and its members.

Restrictions on borrowings - Section 30 of the Central Act further puts restriction on borrowings. According to this section, a registered society shall accept loans and deposits from persons who are not members subject to the restrictions and limits of the bye-laws of the society. The auditor will have to examine the bye-laws in this respect.

Investment of funds - According to section 32 of the Central Act, a society may invest its funds in any one or more of the following:

a. In the Central or State Co-operative Bank.

b. In any of the securities specified in section 20 of the Indian Trusts Act, 1882.

c. In the shares, securities, bonds or debentures of any other society with limited liability.

d. In any co-operative bank, other than a Central or State co-operative bank, as approved by the Registrar on specified terms and conditions.

e. In any other moneys permitted by the Central or State Government.

In the principal provision relating to the investments of funds of a co-operative society, the Central as well as State Acts does not mention anything about the investment of reserve fund outside the business specifically.

Appropriation of profits - According to section 33 of the Central Act, a prescribed percentage of the profits should be transferred to Reserve Fund, before distribution as dividends or bonus to members.

Contributions to Charitable Purposes - According to section 34, a registered society may, with the sanction of the Registrar, contribute an amount not exceeding 10% of the net profits remaining after the compulsory transfer to the reserve fund for any charitable purpose as defined in section 2 of the Charitable Endowments Act, 1890.

Investment of Reserve Fund outside the business or utilisation as working capital - Some of the State Acts provide that a society may use the Reserve Fund:

a. In the business of a society, as working capital (subject to the rules made in this behalf).

b. May invest as per provisions of the Act.

c. May be used for some public purposes likely to promote the object of the society. The auditor should ensure strict compliance with the State Act and Rules in this regard.

Contribution to Education Fund - Some of the State Acts provide that every society shall contribute annually towards the Education Fund of the State Federal Society, at the appropriate rate as per the class of the society. Contribution to Education Fund is a charge on profits and not an appropriation.

Apart from statutory provisions relating to Reserve Fund, the auditor may have regard to the provisions in bye-laws and Rules and Regulations of the society regarding the appropriation of profits. Transfers to other reserves, dividends to members etc. are the other appropriations. Appropriations of profits must be approved by the General Body of the society, which is the supreme authority in the co-operative management. Further, it may be noted that necessary accounting entries for the appropriation of profits must be passed after the date of approval by the General Body. Here there is a departure from corporate accounting practice, where entries are passed for proposed appropriations, subject to approval of Annual General Meeting.

According to certain State Acts, transfers to Dividend Equalization Reserve and Share Capital Redemption Fund are stated as charges against profits. According to the generally accepted principles of accountancy these items are not charges, but appropriation of profits. The auditor should point out such spots where statutory provisions of any law are in contradiction with the generally accepted accounting principles.

Valuation of Assets and Liabilities - Regarding valuation of assets there are no specific provisions or instructions under the Act and Rules and as such due regard shall be had to the general principles of accounting and auditing conventions and standards adopted. The auditor will have to ascertain existence, ownership and valuation of assets. Fixed assets should be valued at cost less adequate provision for depreciation. The incidental expenses incurred in the acquisition and the installation expenses of assets should be properly capitalised. If the difference in the original cost of acquisition and the present market price is of far reaching significance, a note regarding the present market value may be appended; so as to have a proper disclosure in the light of present inflatory conditions. The current assets be valued at cost or market price, whichever is lower. Regarding the liabilities, the auditor should see that all the known liabilities are brought into the account, and the contingent liabilities are stated by way of a note.

Adherence to Co-operative Principles - The auditor will have to ascertain in general, how far the objects, for which the co-operative organisation is set up, have been achieved in the course of its working. The assessment is not necessarily in terms of profits, but in terms of extending of benefits to members who have formed the society. Considered from the viewpoint of social benefits it may be looked into that how far the sales could be affected at lower prices. For the achievement of these activities, cost accounting methods, store control methods, techniques of standard costing, budgetary control etc. should be adopted. However, these modern techniques are mostly not in application and as such in practice a wide gap is found in the goals to be achieved and the actual achievements. While auditing the expenses, the auditor should see that they are economically

incurred and there is no wastage of funds. Middlemen commissions are, as far as possible, avoided and the purchases are made by the committee members directly from the wholesalers. The principles of propriety audit should be followed for the purpose.

Observations of the Provisions of the Act and Rules - An auditor of a co-operative society is required to point out the infringement with the provisions of Co-operative Societies Act and Rules and bye-laws. The financial implications of such infringements should be properly assessed by the auditor and they should be reported. Some of the State Acts contain restrictions on payment of dividends, which should be noted by the auditor.

Verification of Members' Register and examination of their pass books - Examination of entries in members pass books regarding the loan given and its repayments, and confirmation of loan balances in person is very much important in a co-operative organisation to assure that the entries in the books of accounts are free from manipulation. Specifically in the rural and agricultural credit societies, members are not literate and as such this is a good safeguard on their part. Of course this checking will be resorted to on a test basis, which is a matter of judgement of the auditor.

Special report to the Registrar - During the course of audit, if the auditor notices that there are some serious irregularities in the working of the society he may report these special matters to the Registrar, drawing his specific attention to the points. The Registrar on receipt of such a special report may take necessary action against the society. In the following cases, for instance, a special report may become necessary:

i. Personal profiteering by members of managing committee in transactions of the society, which are ultimately detrimental to the interest of the society.

ii. Detection of fraud relating to expenses, purchases, property and stores of the society.

iii. Specific examples of mis-management. Decisions of management against cooperative principles.

iv. In the case of urban co-operative banks, disproportionate advances to vested interest groups, such as relatives of management, and deliberate negligence about the recovery thereof. Cases of reckless advancing, where the management is negligent about taking adequate security and proper safeguards for judging the credit worthiness of the party.

Audit classification of society - After a judgement of an overall performance of the society, the auditor has to award a class to the society. This judgement is to be based on the criteria specified by the Registrar. It may be noted here that if the management of the society is not satisfied about the award of audit class, it can make an appeal to the Registrar, and the Registrar may direct to review the audit classification. The auditor should be very careful, while making a decision about the class of society.

Discussion of draft audit report with managing committee - On conclusion of the audit, the auditor should ask the Secretary of the society to convene the managing committee meeting to discuss the audit draft report. The audit report should never be finalised without discussion with the managing committee. Minor irregularities may be got settled and rectified. Matters of policy should be discussed in detail.

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN PUBLIC SECTOR UNDERTAKINGS

Audit of public enterprises in India is not restricted to financial and compliance audit; it extends also to efficiency, economy and effectiveness with which these operate and fulfil their objectives and goals. Another aspect of such audit relates to questions of propriety; this audit is directed towards an examination of management decisions in sales, purchases, contracts, etc. to see whether these have been taken in the best interests of the undertaking and conform to accepted principles of financial propriety.

Public enterprises have been setup with socio-objectives. An objective assessment with reference to such objectives' fulfillment would require comprehensive audit. The starting point of a comprehensive audit of a public enterprise, which covers aspects of economy, efficiency and effectiveness, is the preparation of an audit

programme based on the study of decisions relating to the setting up of the enterprise, its objectives, the areas of operation, organisation, financial and operational details available in the annual reports and accounts, capital and operational budgets, deliberations of the board of directors, material in the earlier audit inspection reports on the enterprise and other relevant available papers.

These audit programmes (or guidelines) identify the areas/aspects which require further detailed audit analysis and criteria, the data required for such analysis and the sources of such data, the extent of the audit analysis including the test checks to be applied and the instructions to the audit parties assigned to the work.

The areas covered are those of investment decisions, project formulation and management, organisation, delegation of powers and management information systems, organisational effectiveness, capacity utilisation, management of equipment, plant and machinery, production performance, use of materials, productivity of labour, idle capacity, costs and prices, development of complementary ancillary small scale industries, materials management, sales and credit control, budgetary and internal control systems, etc.

The areas covered in audit will naturally vary from enterprise to enterprise depending on the nature of the enterprise, its objectives and operations. Some of the broad areas are listed below:

- Comparison of overall capital cost of the project with the approved planned costs.
- Production or operational outputs vis-a-vis under-utilisation of the installed capacity.
- Systems of project formulation and implementation.
- Cost control measures.
- Research and development programmes.
- System of repairs and maintenance.

SPECIAL POINTS RELATING TO INTERNAL AUDIT OF PARTNERSHIP FIRMS / LLPS

The internal auditors should examine the partnership agreement and note the provisions therein as regards the following matters:

1. The name and style under which the business shall be conducted.
2. The duration of the partnership, if any, that has been agreed upon.
3. The amount of capital that shall be contributed by each partner-whether it will be fixed or could be varied from year to year.
4. The period at the end of which the accounts of the partnership will be closed periodically and the proportions in which the profit shall be divided among the partners or losses shall have to be contributed by them; whether the losses shall be borne by the partners or whether any of the partners will not be required to do so.
5. The provisions as regards maintenance of books of account and the matters which must be taken into account for determining the profits of the firm available for division among the partners e.g., creation of reserves, provision for depreciation, etc.
6. Borrowing capacity of the partnership (when it is not implied as in the case of non-trading firms).
7. The rate at which interest will be allowed on the capitals and loans provided by partners and the rate at which it will be charged on their drawings and current accounts.
8. Whether any salaries are payable to the partners or withdrawals are permitted against shares of profits and, if so, to what extent?

9. Duties of the partners as regards the management of business of the firm; also, the partners who shall act as managing partners.
10. Who shall operate the bank account of the firm? How will the surplus funds of the partnership be invested?
11. Limitations and restrictions that have been agreed upon, the rights and powers of partners and on their implied authority to pledge the firm's credit or to render it liable.

Matters which should be specially considered in the audit of accounts of a partnership:

1. Confirming that the letter of appointment, signed by a partner, duly authorized clearly states the nature and scope of audit contemplated by the partners, specially the limitation, if any, under which the auditor shall have to function.
2. Studying the minute book, if any, maintained to record the policy decision taken by partners specially the minutes relating to authorisation of extraordinary and capital expenditure, raising of loans; purchase of assets, extraordinary contracts entered into and other such matters as are not of a routine nature.
3. Verifying that the business in which the partnership is engaged is authorised by the partnership agreement; or by any extension or modification thereof agreed to subsequently.
4. Examining whether books of account appear to be reasonable and are considered adequate in relation to the nature of the business of the partnership.
5. Verifying generally that the interest of no partner has suffered prejudicially by an activity engaged in by the partnership which, it was not authorised to do under the partnership deed or by any violation of a provision in the partnership agreements.
6. Confirming that a provision for the firm's tax payable by the partnership has been made in the accounts before arriving at the amount of profit divisible among the partners.
7. Verifying that the profits and losses have been divided among the partners in their agreed profit-sharing ratio.

SPECIAL POINTS RELATING TO INTERNAL AUDIT OF SHIPPING COMPANIES

The following points need to be considered while conducting audit of Shipping Company –

- As per appointment letter, Auditor should know the scope of his audit work along with legal requirements to prepare his audit Program accordingly.
- Study the Articles of Association.
- Also study the contracts between Captains of ship and third parties.
- Thoroughly study the internal control system and should prepare his audit Program accordingly.
- Ensure that separate account has to be maintained for each voyage.
- Verify that all revenue expenses are to be charged to Voyage account and all incomes should be credited to Voyage account.
- Separate ledger account for each voyage should be maintained.
- Transactions relating to foreign exchange must be duly incorporated in the books of accounts.
- Ask for advices from agents and receiving officers to vouch freight charges paid. He should also verify the provisions relating to outstanding freight amount.

- Proper depreciation should be charged for each ship.
- Verify the rates of freight, commission and brokerage etc.
- Proper allocation of insurance premium of each voyage is very much important. Balance amount of unexpired insurance should be carried forward. The claim received on account of insurance should also be properly accounted for.
- Proper adjustment and accounting is must for outstanding liabilities and assets.
- Ensure that the capital expenditure should not be charged to revenue account and vice versa.
- Heavy amount of repair and expenditure should be treated as deferred revenue expenditure.
- Verify the title deed of ships and other related documents on account of purchase of ships.

SPECIAL POINTS RELATING TO INTERNAL AUDIT OF ELECTRIC SUPPLY COMPANY

The following points need to be considered by an Auditor while conducting Audit of Electricity Supply Company:

- Study the internal control system related to billing, payment collection, collection of debts and payments of wages, electricity charges, etc.
- Well versed with the Provisions of Electricity (Supply) Act, 1948 and the Indian Electricity Act, 1910.
- Go through the Memorandum and Articles of Association, if any, specially noting the provisions relating to accounts.
- Verify the bills issued to consumers.
- Verify tabular ledger of consumers with original records.
- Verify the receipt of cash from cash receipt counterfoils, cash book, bank book.
- Examine the total number of bills generated, payment received and pending for payments.
- Verify whether late deposit bills are paid inclusive of late payment charges?
- Verify whether proper accounting is done for arrear of bills.
- Payment received on account of arrears should be properly accounted for.
- Proper accounting should be done according to the revenue and capital expenditure.
- Vouch payment for repair of sub-power stations, transformers and meters; all these repairs should be treated as revenue expenses.
- All allowances and rebates should be properly sanctioned by the appropriate authority.
- All accounting forms should be according to the requirements of the Act.
- Depreciation should be properly verified according to applicable provisions of the Act.

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN HOTELS

The special considerations in a hotel audit can be summarised as follows:

1. **Internal Controls -** Pilfering is one of the greatest problems in any hotel and the importance of internal control cannot be undermined. It is the responsibility of management to introduce controls which will minimise the leakage as far as possible. Evidence of their success is provided by the preparation of regular perhaps weekly, trading accounts for each sales point and a detailed scrutiny of

the resulting profit percentages, with any deviation from the anticipated form being investigated. The auditor should obtain these regular trading accounts for the period under review, examine them and obtain explanations for any apparent deviations.

If the internal control in a hotel is weak or perhaps breaks down, then a very serious problem exists for the auditor. As a result of the transient nature of many of his clients' records, the auditor must rely to a very large extent on the gross margin shown by the accounts. As a result, the scope of his audit tests will necessarily be increased and, in the event of a material margin discrepancy being unexplained, he will have to consider qualifying his audit report.

2. **Room Sales -** The charge for room sales is normally posted to guest bills by the receptionist/ front office or in the case of large hotels by the night auditor. The source of these entries is invariably the guest register and audit tests should be carried out to ensure that the correct numbers of guests are charged for the correct period. Any difference between the charged rates used on the guests' bills and the standard room rate should be investigated to ensure that they have been properly authorised.

   In many hotels, the housekeeper prepares a daily report of the rooms which were occupied the previous night and the number of beds kept in each room. This report tends not to be permanently retained and the auditor should ensure that a sufficient number of reports are available for him to test both with the guest register and with the individual guest's bill.

3. **Inventories -** The inventories in any hotel are both readily portable and saleable particularly the food and beverage inventories. It is therefore extremely important that all movements and transfers of such inventories should be properly documented to enable control to be exercised over each individual stores areas and sales point. The auditor should carry out tests to ensure that all such documentation is accurately processed.

   Areas where large quantities of inventory are held should be kept locked, the key being retained by the departmental manager. The key should be released only to trusted personnel and unauthorised persons should not be permitted in the stores areas except under constant supervision. In particular, any movement of goods in or out of the stores should be checked. Many hotels use specialised professional valuers to take and value the inventories on a continuous basis throughout the year. Such a valuation is then almost invariably used as the basis of the balance sheet inventory figure at the year end. Although such valuers are independent of the audit client, it is important that the auditor satisfies himself that the amounts included for such inventories are reasonable. In order to satisfy himself of this, the auditor should consider attending the physical inventory taking and carrying out certain pricing and calculation tests. The extent of such tests could well be limited since the figures will have been prepared independently of the hotel.

4. **Fixed Assets -** The accounting policies for fixed assets of individual hotels are likely to differ. However, many hotels account for certain quasi-fixed assets such as silver and cutlery on inventory basis. This can lead to confusion between each inventory items and similar assets which are accounted for on a more normal fixed assets basis. In such cases, it is important that very detailed definitions of inventory items exist and the auditor should carry out tests to ensure that the definitions have been closely followed.

5. **Casual Labour -** The hotel trade operates to very large extent on casual labour. The records maintained of such wage payments are frequently inadequate. The auditor should ensure that defalcation on this account does not take place by suggesting proper controls to the management.

6. **Other points**

   i. For ledgers coming through travel agents or other booking agencies the bills are usually made on the travel agents or booking agencies. The auditor should ensure that money are recovered from the travel agents or booking agencies as per the terms of credit allowed.

ii. Commission, if any, paid to travel agents or booking agents should be checked by reference to the agreement on that behalf.

iii. The auditor should ensure that proper records re-maintained for booking of halls and other premises for special parties and recovered on the basis of the tariff.

iv. The auditor should verify a few restaurant bills by reference to K.O.T.s (Kitchen Order Tickets) or basic record. This would enable the auditor to ensure that controls regarding revenue cycle are in order.

v. The auditor should see that costs of repairs and minor renovation and redecoration are treated as revenue expenditure, whereas costs of major alterations and additions to the hotel building and facilities capitalised.

vi. The auditor should ensure that proper valuation of occupancy-in-progress at the balance sheet date is made and included in the accounts.

vii. The auditor should satisfy himself that all taxes collected from occupants on food and occupation have been paid over to the proper authorities

SPECIAL POINTS RELATING TO INTERNAL AUDIT IN HOSPITALS

1. **Register of Patients:** Vouch the Register of patients with copies of bills issued to them. Verify bills for a selected period with the patients' attendance record to see that the bills have been correctly prepared. Also see that bills have been issued to all patients from whom an amount was recoverable according to the rules of the hospital.

2. **Collection of Cash:** Check cash collections as entered in the Cash Book with the receipts, counterfoils and other evidence for example, copies of patients bills, counterfoils of dividend and other interest warrants, copies of rent bills, etc.

3. **Income from Investments, Rent etc:** See by reference to the property and Investment Register that all income that should have been received by way of rent on properties, dividends, and interest on securities have been collected.

4. **Legacies and Donations:** Ascertain that legacies and donations received for a specific purpose have been applied in the manner agreed upon.

5. **Reconciliation of Subscriptions:** Trace all collections of subscription and donations from the Cash Book to the respective Registers. Reconcile the total subscriptions due (as shown by the Subscription Register and the amount collected and that still outstanding).

6. **Authorisation and Sanctions:** Vouch all purchases and expenses and verify that the capital expenditure was incurred only with the prior sanction of the Trustees or the Managing Committee and that appointments and increments to staff have been duly authorized.

7. **Grants and TDS:** Verify that grants, if any, received from Government or local authority has been duly accounted for. Also, that refund in respect of taxes deducted at source has been claimed.

8. **Budgets:** Compare the totals of various items of expenditure and income with the amount budgeted for them and report to the Trustees or the Managing Committee, significant variations which have taken place.

9. **Internal Check:** Examine the internal check as regards the receipt and issue of stores; medicines, linen, apparatus, clothing, instruments, etc. so as to insure that purchases have been properly recorded in the Inventory Register and that issues have been made only against proper authorisation.

10. **Depreciation:** See that depreciation has been written off against all the assets at the appropriate rates.

11. **Registers:** Inspect the bonds, share scrips, title deeds of properties and compare their particulars with those entered in the property and Investment Registers.

12. **Inventories:** Obtain inventories, especially of stocks and stores as at the end of the year and check a percentage of the items physically; also compare their total values with respective ledger balances.

13. **Management Representation and Certificate:** Get proper Management Representation and Certificate with respect to various aspects covered during the course of audit.

PRACTICE QUESTIONS

Illustration 1:

Mention the special points to be examined by the auditor in the audit of a charitable institution running hostel for students pursuing the CS Course and which charges only Rs. 500 per month from a student for his lodging/boarding.

Solution:

1. **General**
   - i. Study the constitution under which the charitable institution has been set up whether under the Society Registration Act, as a trust or as a company limited by guarantee. Verify whether it is managed as contemplated by the law and rules and regulations made thereunder.
   - ii. Examine the internal control structure particularly with reference to admission to hostel, expenses incurred on different kinds of activities.
   - iii. Verify the broad nature of expenses likely to be incurred with reference to the previous year's annual audited accounts.
2. **Verification of the receipts**
   - i. Check the amounts received on account of, monthly rentals, etc., and receipts issued for the same.
   - ii. Ascertain that there is adequate internal control over the issue of official receipts, custody of unused receipt books, printing of receipt books, etc.
   - iii. Cross - tally the rent received along with the number of students (from the student register) staying in the hostel during the year.
3. **Verification of expenses**
   - i. Check the day-to-day administration expenses incurred along with the necessary vouchers, supporting for the same like salary registers, repairs register, etc.
   - ii. Verify whether the expenses incurred are in conformity with the budgets prepared internally or filed with the relevant authorities.
4. Verify investments made from surplus funds as well as existing investments by physically verifying the same and that they are in the name of the institution and that there is no charge/pledge against the same.
5. Verify all capital expenditure and expenditure on repairs, etc., incurred with the vouchers and also whether proper tenders, etc., were invited for the same. See that all furniture, glass, cutlery, kitchen utensils, liner, etc. are adequately depreciated.

Illustration 2:

An NGO operating in Delhi had collected large scale donations for Tsunami victims. The donations so collected were sent to different NGOs operating in Tamil Nadu for relief operations. This NGO operating in Delhi has appointed you to audit its accounts for the year in which it collected and remitted donations for Tsunami victims. Draft audit programme for audit of receipts of donations and remittance of the collected amount to different NGOs. Mention six points each, peculiar to the situation, which you will like to incorporate in your audit programme for audit of said receipts and remittances of donations.

Solution:

Receipt of Donations:

i. Internal Control System: Existence of internal control system particularly with reference to division of responsibilities in respect of authorised collection of donations, custody of receipt books and safe custody of money.

ii. Custody of Receipt Books: Existence of system regarding issue of receipt books, whether unused receipt books are returned and the same are verified physically including checking of number of receipt books and sequence of numbering therein.

iii. Receipt of Cheques: Receipt Book should have carbon copy for duplicate receipt and signed by a responsible official. All details relating to date of cheque, bank's name, date, amount, etc. should be clearly stated.

iv. Bank Reconciliation: Reconciliation of bank statements with reference to all cash deposits not only with reference to date and amount but also with reference to receipt book.

v. Cash Receipts: Register of cash donations to be vouched more extensively. If addresses are available of donors who had given cash, the same may be cross-checked by asking entity to post thank you letters mentioning amount, date and receipt number.

vi. Foreign Contributions, if any, to receive special attention to compliance with applicable laws and regulations.

Remittance of Donations to Different NGOs:

i. Mode of Sending Remittance: All remittances are through account payee cheques. Remittances through Demand Draft would also need to be scrutinised thoroughly with reference to recipient.

ii. Confirming Receipt of Remittance: All remittances are supported by receipts and acknowledgements.

iii. Identity: Recipient NGO is a genuine entity. Verify address, 80G Registration Number, etc.

iv. Direct Confirmation Procedure: Send confirmation letters to entities to whom donations have been paid.

v. Donation Utilisation: Utilisation of donations for providing relief to Tsunami victims and not for any other purpose.

vi. System of NGOs' Selection: System for selecting NGO to whom donations have been sent.

Illustration 3:

Central Govt. hold 55% of the paid up share Capital in Kisan Credit Co-operative Society, which is incurring huge losses. Advise when the Central Government can direct Special Audit under Section 77 of the Multi State Co-operative Society Act.

Solution:

Central Government shall order for special audit only if that Government or the State Government either by itself or both hold fifty-one percent or more of the paid-up share capital in such Multi -State co-operative society. Under section 77 of the Multi-State Co-operative Societies Act, 2002, where the Central Government is of the opinion:

i. that the affairs of any Multi-State co-operative society are not being managed in accordance with self-help and mutual deed and co-operative principles or prudent commercial practices or with sound business principles; or

ii. that any Multi-State co-operative society is being managed in a manner likely to cause serious injury or damage to the interests of the trade industry or business to which it pertains; or

iii. that the financial position of any Multi-State co-operative society is such as to endanger its solvency.

Thus, in the given case since Central Govt is holding 55% shares and financial position of Kisan Credit co-operative society is in danger, Central government can direct for special audit.

Illustration 4:

The general transactions of a hospital include patient treatment, collection of receipts, donations, capital expenditures. You are required to mention special points of consideration while auditing such transactions of a hospital?

Solution:

Special points of consideration while auditing certain transactions of a hospital are stated below-

Register of Patients: Vouch the Register of patients with copies of bills issued to them. Verify bills for a selected period with the patients' attendance record to see that the bills have been correctly prepared. Also see that bills have been issued to all patients from whom an amount was recoverable according to the rules of the hospital.

Collection of Cash: Check cash collections as entered in the Cash Book with the receipts, counterfoils and other evidence for example, copies of patients bills, counterfoils of dividend and other interest warrants, copies of rent bills, etc.

Legacies and Donations: Ascertain that legacies and donations received for a specific purpose have been applied in the manner agreed upon.

Reconciliation of Subscriptions: Trace all collections of subscription and donations from the Cash Book to the respective Registers. Reconcile the total subscriptions due (as shown by the Subscription Register and the amount collected and that still outstanding).

Authorisation and Sanctions: Vouch all purchases and expenses and verify that the capital expenditure was incurred only with the prior sanction of the Trustees or the Managing Committee and that appointments and increments to staff have been duly authorised.

Illustration 5:

As an internal auditor, what would be your areas of consideration while auditing the element of Room Sales during the audit of a 5-Star Hotel.

Solution:

Following points merit consideration while auditing the element of ROOM SALES during the audit of a Hotel:

a. The charge for room sales is normally posted to guest bills by the receptionist/ front office or in the case of large hotels by the night auditor.

b. The source of these entries is the guest register and audit tests should be carried out to ensure that the correct numbers of guests are charged for the correct period.

c. Any difference between the charged rates used on the guests' bills and the standard room rate should be investigated to ensure that they have been properly authorised.

d. In many hotels, the housekeeper prepares a daily report of the rooms which were occupied the previous night and the number of beds kept in each room. This report tends not to be permanently retained and the auditor should ensure that a sufficient number of reports are available for him to test both with the guest register and with the individual guest's bill.

e. Ensure compliance with the provisions of FEMA and RBI if receipts are in foreign currency. Ensure application of proper Conversion rate.

f. Special emphasis to be laid on receipts through Credit Cards.

g. The auditor should ensure that proper valuation of occupancy-in-progress at the balance sheet date is made and included in the accounts.

Illustration 6:

You have been appointed as an auditor of an NGO, briefly state the points on which you would concentrate while planning the audit of such an organisation?

Solution:

While planning the audit of an NGO, the auditor may concentrate on the following:

a) Knowledge of the NGO's work, its mission and vision, areas of operations and environment in which it operate.

b) Updating knowledge of relevant statutes especially with regard to recent amendments, circulars, judicial decisions related to the statutes.

c) Reviewing the legal form of the Organisation and its Memorandum of Association, Articles of Association, Rules and Regulations.

d) Reviewing the NGO's Organisation chart, then Financial and Administrative Manuals, Project and Programme Guidelines, Funding Agencies Requirements and formats, budgetary policies if any.

e) Examination of minutes of the Board/Managing Committee/Governing Body/Management and Committees thereof to ascertain the impact of any decisions on the financial records.

f) Study the accounting system, procedures, internal controls and internal checks existing for the NGO and verify their applicability.

g) Setting of materiality levels for audit purposes.

h) The nature and timing of reports or other communications.

i) The involvement of experts and their reports.

j) Review the previous year's Audit Report.

Illustration 7:

State the points which merit consideration in the audit of a CLUB w.r.t its members.

Solution:

The points which merit consideration in the audit of a CLUB w.r.t its members:-

(1) Entrance Fee- Vouch the receipt on account of **entrance fees** with –

- members' applications and counterfoils issued to them,
- on a reference to minutes of the Managing Committee.

(2) Member Subscriptions- Vouch members' subscriptions with –

- the counterfoils of receipt issued to them,
- trace receipts for a selected period to the Register of Members,
- Also reconcile the amount of total subscriptions due with the amount collected and that outstanding.

(3) Subscription Arrears/in Advance- Ensure that –

- arrears of subscriptions for the previous year have been correctly brought over,
- arrears for the year under audit and subscriptions received in advance have been correctly adjusted.
- Subscriptions received in advance should have been properly accounted for.

(4) Arithmetical accuracy- Check totals of various columns of the Register of members and tally them across.

(5) Register of Members- See the **Register of Members** to ascertain –

- the Member's dues which are in arrear,
- enquire whether necessary steps have been taken for their recovery, and
- the amount considered irrecoverable should be mentioned in the Audit Report.

(6) Member Accounts- Trace debits for a selected period from subsidiary registers maintained in respect of supplies and services to members to confirm that the account of every member has been debited with amounts recoverable from him.

LESSON ROUND-UP

- Banking Industry in India is regulated by the Reserve Bank of India (RBI) known as the Central Bank. The lesson covers Major functions and responsibilities of RBI, Regulatory Framework of Banking Company and Major areas to be covered under Audit while conducting audit of banking company.
- An Indian insurance company is formed and registered under the Companies Act, 2013 and the aggregate holdings of equity shares by a foreign company, either by itself or through its subsidiary companies or its nominees, do not exceed twenty-six per cent of the paid-up equity capital of such Indian insurance company. The sole objects of the Indian Insurance Company shall be to carry on life insurance business or general insurance business or re-insurance business.
- Major areas to be covered under Audit while conducting audit of insurance company such as verification of premiums, claims, commission, operating expenses, investments, cash and bank balances etc.
- Co-operative society is a business organisation with a special mode of doing business, by pulling together all the means of production co-operatively, elimination of middlemen and exploitation from outside forces.
- Major areas to be covered under Audit while conducting audit of Co-operative society such as Contributions to Charitable Purposes, Valuation of Assets and Liabilities, Adherence to Co-operative Principles, Observations of the Provisions of the Act and Rules, Verification of Members' Register and examination of their pass books, Special report to the Registrar etc.
- Audit of public enterprises in India is not restricted to financial and compliance audit; it extends also to efficiency, economy and effectiveness with which these operate and fulfil their objectives and goals. Another aspect of such audit relates to questions of propriety; this audit is directed towards an examination of management decisions in sales, purchases, contracts, etc. to see whether these have been taken in the best interests of the undertaking and conform to accepted principles of financial propriety. Some of the major areas of audit includes, Comparison of overall capital cost of the project with the approved planned costs, Production or operational outputs vis-a-vis under-utilisation of the installed capacity, Systems of project formulation and implementation, Cost control measures etc.
- Special Points relating to internal audit of Partnership Firms / LLPs, Shipping Company, Electricity Supply Company etc.
- Special Points relating to internal audit of Hotels such as Internal Controls, Room Sales, Inventories, Fixed Assets, Casual Labour etc. Special Points relating to internal audit of Hospital such as Register of Patients, Collection of Cash, Income from Investments, Legacies and Donations, Reconciliation of Subscriptions, Grants, Budget, Registers, Inventories etc.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. You have been appointed as an auditor of an NGO, briefly state the points on which you would concentrate while planning the audit of such an organisation?
2. The general transactions of a hospital include patient treatment, collection of receipts, donations, capital expenditures. You are required to mention special points of consideration while auditing such transactions of a hospital?

3. As an internal auditor, what would be your areas of consideration while auditing the element of ROOM SALES during the audit of a 7 Star hotel?
4. Mention any four special points which you as an internal auditor would look while auditing the books of a partnership firm.
5. You have been appointed as an auditor of an NGO briefly state the points on which you would concentrate while planning the audit of such an organization?
6. What are the steps involved in audit of educational institutions.
7. RCM College, an institution managed by a trust, has received a grant of Rs. 2.5 crore from Government nodal agencies for funding a project of research on rural health systems in India. Draft an audit questionnaire for auditing this fund.
8. State the steps would be taken into consideration in auditing the receipts from patients of a hospital?
9. State any five special points which you, as an auditor, would look into while examining the income and collection of fund by an NGO engaged in providing relief work for flood victims.
10. Mention any six points to be considered for good internal control for collection of tuition fees from students of college.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's

- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Reporting under Internal Audit

Lesson 8

KEY CONCEPTS

■ Internal Audit Report ■ Internal Audit Checklist ■ CARO 2020

Learning Objectives

To understand:

- The reporting under Internal Audit
- The objectives of Reporting under Internal Audit
- Important aspects of quality reporting under Internal Audit
- Who are the users of Internal Audit Report?
- Layout of Internal Audit Report
- What are the precautions to be taken care of while drafting Internal Audit Report?
- Communication of outcomes of Internal Audit to Management
- Checklist of Internal Audit Report
- Reporting under various clauses of Companies Audit Report Order 2020 [CARO 2020]

Lesson Outline

- Introduction
- The objectives of Reporting
- Important aspects of quality reporting
- Layout of Internal Audit Report
- Communication to Management
- Internal Audit Report Checklist
- CARO – Companies (Auditors Report) Order
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION

The essential part of internal audit is the dissemination of the results of internal audit and reports the findings to management, and those charged with governance. The internal audit report of the company is a significant aspect which throws light on any kind of non-compliance with the regulations that are needed to be kept in mind. It also highlights the aspects which need to be improved.

The internal auditor should review and assess the analysis drawn from the internal audit evidence obtained as the basis for his conclusion on the efficiency and effectiveness of systems, processes and controls including items of financial statements.

Standard on Internal Audit (SIA) 4 "Reporting" issued by the Internal Audit Standards Board of ICAI specifies that the internal auditor's report should contain a clear written expression of significant observations, suggestions/ recommendations based on the policies, risks, controls and transaction processing taken as a whole and management responses. The process of reporting flows from overall internal audit objectives, as specified in the appointment letter.

Objectives of Reporting

The objectives of issuing Internal Audit Reports on significant internal audit assignments are to:

(a) Share with the auditee, details of all significant findings based on audit procedures undertaken;

(b) Allow management to understand the issues and take corrective actions;

(c) Leads to improved performance and control framework;

(d) The follow-up process monitors the progress of agreed upon management action plans and reports this progress to senior management and the audit committee.

The overall objective of reporting results is to highlight the effectiveness of internal controls and risk management processes to enhance governance in line with the Internal Audit Charter.

IMPORTANT ASPECTS OF QUALITY REPORTING

Internal auditor should draft a high-quality report presenting his audit findings and recommendations in the best presentable form, so that timely and relevant information is delivered to key stakeholders. Enhancing the quality of internal audit report would assist to achieve the objective of internal audit by providing relevant assurance and contributing to the efficiency and effectiveness of governance, risk management and control. Internal auditor should share their opinion on the matters that were of most significance in the audit of the current period. Qualitative internal audit report can further support the governance role of the audit committee by creating a better link between the role of the internal audit and the responsibilities of the audit committee and board.

Internal audit report should be compact and easy to read, understandable to a broad audience. Internal audit report should be drafted in such a manner that the readers are easily able to scan an audit finding and take a decision about the corrective steps to be taken. Further, the report should be concrete, descriptive and factual, and it should communicate a precise message. The objectivity in writing report should be maintained and a self-review should be done to ensure that the report is clear, complete and correct.

Users of Internal Audit Report

Generally, the internal audit reports should be drafted taking into account requirements of the various types of readers of the internal audit report which, generally, includes following:

- Board of Directors and Audit Committee

- Senior Management like, CEO, CFO, etc.
- Business Management and Process Owners
- Personnel or Employees tasked with direct implementation of recommendations
- External Auditors
- Other External Stakeholders, like, Regulators.

Accordingly, an analysis of the need and purpose of various readers (stakeholders) of the report would help the internal auditor to appropriately design their report. In conclusion, while drafting the report, the internal auditor should consider the logic of auditing, the analysis of reporting objectives and the analysis of requirement of the readers.

The following are the important aspects which an internal auditor should analyze while drafting internal audit report:

(a) Most important readers of the internal audit report inside and outside the organization;

(b) Knowledge of the subject covered in the report by the readers;

(c) Usage of the report by interested readers;

(d) Readers should accept conclusions and results;

(e) Implementation of recommendations that have both short and long-term impact on issue.

LAYOUT OF INTERNAL AUDIT REPORT

"Reporting" lays down that the internal auditor's report should ordinarily include certain basic elements. An illustrative layout is given below:

(a) Title;

(b) Addressee;

(c) Period of coverage of the Report;

(d) Report Distribution List;

(e) Opening or introductory paragraph:

  i. identification of the processes/functions and items of financial statements audited; and

  ii. a statement of the responsibility of the entity's management and the responsibility of the internal auditor;

(f) Objectives/Scope paragraph (describing the nature of an internal audit):

  i. a reference to the generally accepted audit procedures in India, as applicable;

  ii. a description of the engagement background and the methodology of the internal audit together with procedures performed by the internal auditor; and

  iii. a description of the population and the sampling technique used.

(g) Executive Summary, highlighting the key material issues, observations, control weaknesses and exceptions;

(h) Observations, findings and recommendations made by the internal auditor;

(i) Comments from the local management;

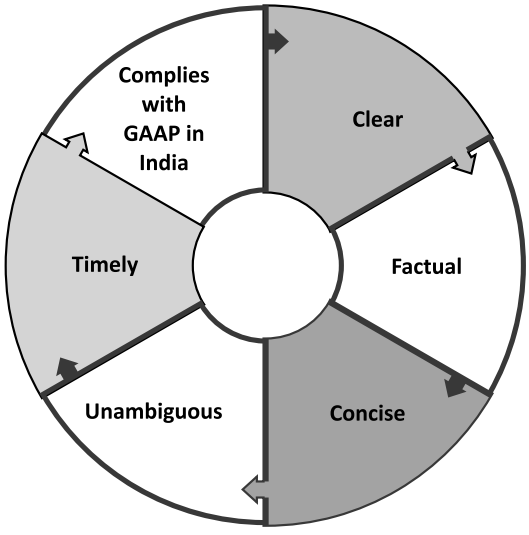
(j) Action Taken Report — Action taken/ not taken pursuant to the observations made in the previous internal audit reports;

(k) Date of the report;

(l) Place of signature; and

(m) Internal auditor's signature with Membership Number.

Internal auditor should take care of following while drafting internal audit report so that the methodology and quality of internal audit report is highlighted to audit committee and other stakeholders:



i. Using the right tone and language;

ii. Taking a positive approach, i.e., tone is not critical, judgmental or unbalanced;

iii. Writing clearly and concisely;

iv. Quality of findings in terms of materiality;

v. Quality of recommendations in terms of impact so that they correct current conditions and prevent future effects;

vi. Degree of risks covered by the internal audit plan;

vii. Root cause analysis of findings which are being carried forward from previous internal audit reports;

viii. Rating recommendations as high, medium and low in order to assist management in assigning priorities. Sometimes, rating as satisfactory, needs improvement and unsatisfactory is also used by internal auditors;

ix. Making report user friendly and streamlining contents to eliminate extraneous or redundant information;

x. Any organizational/ legal constraint or constraint imposed by time and resources should be specified in the report;

xi. Articulating the findings of internal audit and highlighting the risks impacting the organization.

Title of the Report

The internal auditor's report should have an appropriate title expressing the nature of the Report.

Addressee of the Report

The internal auditor's report should be appropriately addressed as required by the circumstances of the engagement. Ordinarily, the internal auditor's report is addressed to the appointing authority or such other person as directed.

Scope Paragraph

The internal auditor's report should describe the scope of the internal audit by stating that the internal audit was conducted in accordance with generally accepted audit procedures as applicable. The management needs this as an assurance that the audit has been carried out in accordance with established Standards.

"Scope" refers to the internal auditor's ability to perform internal audit procedures deemed necessary in the circumstances.

The report should include a statement that the internal audit was planned and performed to obtain reasonable assurance whether the systems, processes and controls operate efficiently and effectively and financial information is free of material misstatement.

The internal auditor's report, in line with the terms of the engagement, should describe the internal audit as including:

a) examining, on a test basis, evidence to support the amounts and disclosures in financial statements;

b) assessing the strength, design and operating effectiveness of internal controls at process level and identifying areas of control weakness, business risks and vulnerability in the system and procedures adopted by the entity;

c) assessing the accounting principles and estimates used in the preparation of the financial statements; and

d) evaluating the overall entity-wide risk management and governance framework.

The Report should include a description of the engagement background, internal audit methodology used and procedures performed by the internal auditor mentioning further that the internal audit provides a reasonable basis for his comments.

Limitation on Scope

When there is a limitation on the scope of the internal auditor's work, the internal auditor's report should describe the limitation.

Executive Summary Paragraph

The Executive Summary paragraph of the internal auditor's report should clearly indicate the highlights of the internal audit findings, key issues and observations of concern, significant controls lapses, failures or weaknesses in the systems or processes.

Observations (Main Report) Paragraph

The Observations paragraph should clearly mention the process name, significant observations, findings, analysis and comments of the internal auditor.

Comments from Local Management

The Comments from Local Management Paragraph should contain the observations and comments from the local management of the entity provided after giving due cognizance to the internal auditor's comments. This should also include local management's action plan for resolution of the issues and compliance to the internal auditor's recommendations and suggestions on the areas of process and control weakness/ deficiency. The management action plan, should contain, inter alia:

a) the timeframe for taking appropriate corrective action;

b) the person responsible; and

c) resource requirements, if any, for ensuring such compliance.

Further comments from the internal auditor, in response to the auditee feedback, are to be clearly mentioned. This paragraph should also contain the internal auditor's suggestions and recommendations to mitigate risks, strengthen controls and streamline processes with respect to each of the observations and comments made.

Action Taken Report Paragraph

The Action Taken Report paragraph should be appended after the observations and findings. It should include:

a) Status of compliance / corrective action already taken / being taken by the auditee with respect to previous internal audit observations;

b) Status of compliance / corrective action not taken by the auditee with respect to previous internal audit observations and the reasons for non-compliance thereof; and

c) Revised timelines for compliance of all open items in (b) above and fixation of the responsibility of the concerned process owner.

Date

The date of an internal auditor's report is the date on which the internal auditor signs the report expressing his comments and observations.

Place of Signature

The report should name the specific location, which is ordinarily the city where the internal audit report is signed.

Internal Auditor's Signature

The report should be signed by the internal auditor in his personal name. The internal auditor should also mention the membership number assigned by the Institute of Chartered Accountants of India in the report so issued by him.

COMMUNICATION TO MANAGEMENT

The internal audit report contains the observations and comments of the internal auditor, presents the audit findings, and discusses recommendations for improvements. To facilitate communication and ensure that the recommendations presented in the final report are practical from the point of view of implementation, the internal auditor should discuss the draft with the entity's management prior to issuing the final report. The different stages of communication and discussion should be as under:

Discussion Draft - At the conclusion of fieldwork, the internal auditor should draft the report after thoroughly reviewing the working papers and the discussion draft before it is presented to the entity's management for

auditee's comments. This discussion draft should be submitted to the entity management for their review before the exit meeting.

Exit Meeting - The internal auditor should discuss with the management of the entity regarding the findings, observations, recommendations, and text of the discussion draft. At this meeting, the entity's management should comment on the draft and the internal audit team should work to achieve consensus and reach an agreement on the internal audit findings.

Formal Draft - The internal auditor should then prepare a formal draft, taking into account any revision or modification resulting from the exit meeting and other discussions. When the changes have been reviewed by the internal auditor and the entity management, the final report should be issued.

Final Report - The internal auditor should submit the final report to the appointing authority or such members of management, as directed. The periodicity of the Report should be as agreed in the scope of the internal audit engagement. The internal auditor should mention in the Report, the dates of discussion draft, exit meeting, Formal Draft and Final Report

INTERNAL AUDIT REPORT CHECKLIST

Assignment Name	***Assignment No***		
	Engagement Manager		
Company Name			
S. No.	***Checklist***	***Status***	***Remarks***
1.	Whether there is an Executive Summary written with summary of high-risk observations for a top management view.		
2.	Whether Objective and Scope Document is given and relates to the Engagement Letter.		
3.	Whether the language used in the Reports are positive, affirmative and objective.		
4.	Whether the language is easily understandable to a general person and jargon free.		
5.	Whether there are no comments which are in an attacking tone and adequate care is taken to keep them free of negative remarks.		
6.	Whether there is adequate numbering system followed and there is a table of contents referring to the report and observations.		
7.	Whether all the observations are supported by evidences and are not ambiguous.		
8.	Are there any trend, Internal Audit Checklist performance information which may be represented using graphs.		
9.	Is caution taken in usage of logos of the clients with adequate written permissions.		

10.	Is the formatting of the report done using standardized formats signed off with the client. Please give extra check on headers, footers, first page, annexure, etc.		
11.	Check whether the valuation of Risk levels is as per the methodology/ score matrix signed off with the client.		
12.	All the observations are linked / mapped to the evidences.		
13.	Ensure that the Audit Report adheres to the Standard of Internal Audit for Reporting issued by Institute of Chartered Accountants of India (ICAI).		
Team Leader Partner		Engagement Manager	

Example

Name of Facility: Admitting and Registration (Healthcare)

Date

Executive Summary

The objective of this review was to obtain an understanding of the key admitting and registration functions managed by the Patient Access Services Department (PAS). During our review, internal controls related to the admitting and registration functions were reviewed and opportunities for improvement were evaluated with a risk significance of low, moderate, or high. Overall Facility Risk Impact and the most significant opportunities for improvement are identified below:

Issue 1: The insurance eligibility software was not always available to the ministry to confirm patient insurance coverage. – **Risk Significance - High**

Issue 2: Insurance pre-certification has not been consistently performed for highdollar scheduled outpatient procedures and surgical cases prior to the initiation of care. **Risk Significance** - **High**

Issue 3: The PAS Department is not confirming patient identification according to the guidelines outlined in Policy. – Verification of Patient Identity. **Risk Significance** - **High**

Issue 4: The PAS department does not check physician suspension lists during inpatient registration to ascertain whether the physician is eligible to admit **Risk Significance** – **High**

Risk of Low Significance – Adequate controls are in place and operating effectively. The audit issues identified are minor or of low significance.

Risk of Moderate Significance – Controls are generally adequate, but major deficiencies with some compensating controls were encountered. A significant number of minor deficiencies may have been noted.

Risk of High Significance – A weakness noted is of sufficient importance to endanger the acceptable function of the activity or to keep a significant objective of the activity from being met. The issue or deficiency adversely impacts, or may adversely impact to a considerable degree, the adequacy of controls or the effectiveness of performance of a significant function of the activity.

Management Response:

Executive ministry management has reviewed evaluation of the internal controls related to the admitting and

registration functions of the PAS Department. Management has acknowledged agreement with the issues contained in this audit report and will implement the following action plans for the most significant risks identified:

Action plan 1: The Healthcare System is currently undergoing an upgrade for the insurance eligibility software. An alternate insurance eligibility method will be determined if the software upgrade fails to perform as required. **Implementation Dates – Within 2 Month**

Action Plan 2: High-dollar scheduled outpatient procedures and surgical cases will be pre-certified according to payer specific guidelines prior to the initiation of care. **Implementation Dates – Within 3 Month**

Action Plan 3: All PAS admitting areas will instruct patients to read back an identifier from the identification band when the band is applied to the patient. **Implementation Dates – Within 1 Month**

Action Plan 4: The PAS Registrars will review the physician suspension listing prior to any inpatient admissions to ensure each physician has current admitting privileges. **Implementation Dates – Within 15 Days**

Additional Comments: Management reviewed a new sample of 10 surgical registrations and noted the following:

1. The software unavailability continues to hinder the eligibility process. THIN is being utilized for insurance eligibility of surgical cases and does not interface with the Meditech system to indicate the eligibility was completed. The pre-admit surgical testing staff will be trained on where to document that the eligibility process was performed.
2. Insurance verification and pre-certification have improved with the employment of additional staff and staff returning from medical leave. Three of the ten cases (all Blue Cross patients) reviewed were not pre-certified. Currently, PFS has a total of five staff responsible for the verification and pre-certification function. The addition of a sixth staff member very soon will enable outpatient Blue Cross and outpatient Medicare patients to be verified and pre-certified.

Additional Procedures and Report Signatures

Based on the above Management Action Plans and the corresponding implementation dates, internal auditor will perform additional follow-up procedures to determine if all action plan steps are implemented in a timely manner. The follow-up procedures will include interviewing key management personnel and observation of supporting documentation where applicable. A status report on the implementation of Management's Action Plan will be presented to the Audit/Corporate Responsibility Committee at regular intervals until all Action Plans have been implemented and/or the issues resolved.

ACCEPTED:

Director of Patient Access Services **Date:**

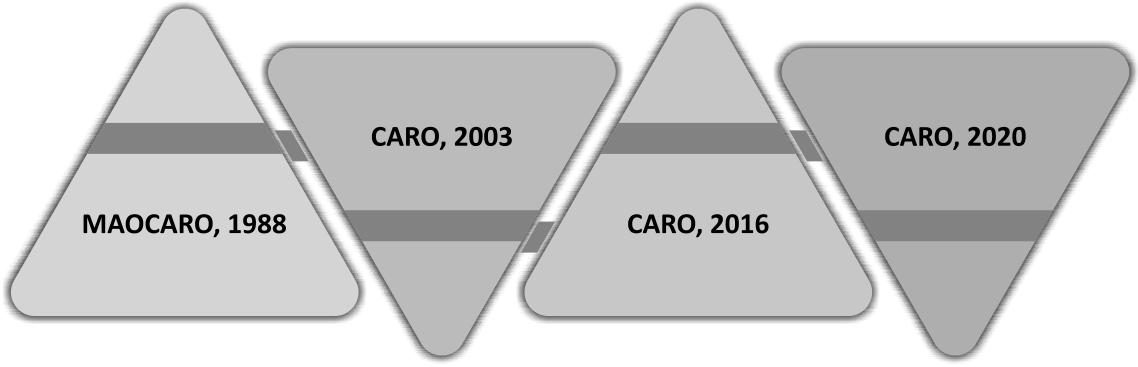
CARO – COMPANIES (AUDITORS REPORT) ORDER

The Central Government, in exercise of the powers conferred under section 227 (4A) of the Companies Act, 1956, had issued CARO, 2003 in June 2003. The Order contained certain matters on which the auditors of companies had to make a statement in their audit report. Thereafter, CARO, 2003 superseded the earlier Order issued in 1988, viz., Manufacturing and Other Companies (Auditor's Report) Order, 1988 (MAOCARO).

It may be worthwhile to note that CARO, 2003 apart from requiring the auditors to report on matters which were included in MAOCARO, 1988 included certain new clauses on which the auditors were now required to make a statement in their audit reports. Some of the significant clauses added, inter alia, by CARO, 2003 required the auditor to report on maintenance of proper inventory records, disposal of significant part of fixed assets of the company affecting the going concern, the use of funds raised by companies through public issues, requiring the auditor to report whether any fraud on or by the company had been noticed or reported during the year under audit, the application of funds raised on short-term basis for long-term purposes, etc. and vice versa.

Thereafter, the Ministry of Corporate Affairs 'MCA', on April 10, 2015, notified the Companies (Auditor's Report) Order, 2015 (CARO, 2015) in supersession of CARO 2003.

Thereafter, the Ministry of Corporate Affairs 'MCA' has issued the Companies (Auditor's Report) Order, 2016 (CARO 2016), on March 29, 2016. This order has been issued in supersession of the Companies (Auditor's Report) Order, 2015, and is applicable for reporting on financial statements of companies whose financial year commences on or after 1st April 2015.



Companies (Auditor's Report) Order, 2020

In order to bring more transparency & faith in Financials Statements of companies, the Ministry of Corporate Affairs introduced the new set of Companies (Auditor's Report) Order, 2020 (CARO 2020). **The CARO, 2020 is applicable for audit of financial statements of eligible companies for the financial years commencing on or after the 1st April, 2021 i.e. 2021-22 onwards.**

The criteria of eligibility of companies on which the CARO, 2020 shall be applicable has not been changed and hence it shall be applicable to all those companies on which CARO, 2016 was applicable. Accordingly CARO 2020 will be applicable to all the companies including foreign companies except the following:

- Banking company,
- Insurance company,
- Section 8 company,
- One Person Company (OPC) [section 2(62)],
- Small company [section 2(85)],
- a private limited company, not being a subsidiary or holding company of a public company, having a paid-up capital and reserves and surplus not more than one crore rupees as on the balance sheet date and which does not have total borrowings exceeding one crore rupees from any bank or financial institution at any point of time during the financial year and which does not have a total revenue as disclosed in Schedule III to the Act, (including revenue from discontinuing operations) exceeding ten crores rupees during the financial year as per the financial statements.

This order stated that every report of the auditor under Section 143 of Companies Act, 2013 must contain the matters stated in 21 clauses as specified under paragraphs 3 and accord reasons for unfavorable or qualified answer as stated in paragraph 4 of CARO 2020.

CARO 2020 will not be applied with respect to auditor's report on Consolidated Financial Statements except clause (xxi) of paragraph 3. The order 2020 elaborated on all the matters which are to be included in the auditor's report.

Clause by Clause Reporting under Companies (Auditor's Report) Order 2020

Matters to be included in the auditor's report are specified in paragraph 3 of the Order. Paragraph 3 has twenty one clauses in all. The clause-wise details of reporting requirement are given below.

CLAUSE (i) PROPERTY, PLANT & EQUIPMENT

a) (A) whether the company is maintaining proper records showing full particulars, including quantitative details and situation of Property, Plant and Equipment;

(B) Whether the company is maintaining proper records showing full particulars of intangible assets;

b) Whether these Property, Plant and Equipment have been physically verified by the management at reasonable intervals; whether any material discrepancies were noticed on such verification and if so, whether the same have been properly dealt with in the books of account;

c) whether the title deeds of all the immovable properties (other than properties where the company is the lessee and the lease agreements are duly executed in favour of the lessee) disclosed in the financial statements are held in the name of the company, if not, provide the details thereof in the format below:-

Description of Property	***Gross Carrying Value***	***Held in name of***	***Whether promoter, director or their relative or employee***	***Period held – indicate range, where appropriate***	***Reason for not being held in name of company***
					*also indicate if in dispute

d) whether the company has revalued its Property, Plant and Equipment (including Right of Use assets) or intangible assets or both during the year and, if so, whether the revaluation is based on the valuation by a Registered Valuer; specify the amount of change, if change is 10% or more in the aggregate of the net carrying value of each class of Property, Plant and Equipment or intangible assets;

e) whether any proceedings have been initiated or are pending against the company for holding any benami property under the Benami Transactions (Prohibition) Act, 1988 and rules made thereunder, if so, whether the company has appropriately disclosed the details in its financial statements.

CLAUSE (ii) INVENTORY & WORKING CAPITAL

a) whether physical verification of inventory has been conducted at reasonable intervals by the management and whether, in the opinion of the auditor, the coverage and procedure of such verification by the management is appropriate; whether any discrepancies of 10% or more in the aggregate for each class of inventory were noticed and if so, whether they have been properly dealt with in the books of account;

b) whether during any point of time of the year, the company has been sanctioned working capital limits in excess of five crore rupees, in aggregate, from banks or financial institutions on the basis of security of current assets; whether the quarterly returns or statements filed by the company with such banks or financial institutions are in agreement with the books of account of the Company, if not, give details.

CLAUSE (iii) DETAILS OF INVESTMENTS, LOANS & ADVANCES

Whether during the year the company has made investments in, provided any guarantee or security or granted

any loans or advances in the nature of loans, secured or unsecured, to companies, firms, Limited Liability Partnerships or any other parties, if so,-

a) whether during the year the company has provided loans or provided advances in the nature of loans, or stood guarantee, or provided security to any other entity [not applicable to companies whose principal business is to give loans], if so, indicate-

   (A) the aggregate amount during the year, and balance outstanding at the balance sheet date with respect to such loans or advances and guarantees or security to subsidiaries, joint ventures and associates;

   (B) the aggregate amount during the year, and balance outstanding at the balance sheet date with respect to such loans or advances and guarantees or security to parties other than subsidiaries, joint ventures and associates.

b) whether the investments made, guarantees provided, security given and the terms and conditions of the grant of all loans and advances in the nature of loans and guarantees provided are not prejudicial to the company's interest;

c) in respect of loans and advances in the nature of loans, whether the schedule of repayment of principal and payment of interest has been stipulated and whether the repayments or receipts are regular;

d) if the amount is overdue, state the total amount overdue for more than ninety days, and whether reasonable steps have been taken by the company for recovery of the principal and interest;

e) whether any loan or advance in the nature of loan granted which has fallen due during the year, has been renewed or extended or fresh loans granted to settle the overdues of existing loans given to the same parties, if so, specify the aggregate amount of such dues renewed or extended or settled by fresh loans and the percentage of the aggregate to the total loans or advances in the nature of loans granted during the year [not applicable to companies whose principal business is to give loans];

f) whether the company has granted any loans or advances in the nature of loans either repayable on demand or without specifying any terms or period of repayment, if so, specify the aggregate amount, percentage thereof to the total loans granted, aggregate amount of loans granted to Promoters, related parties as defined in clause (76) of section 2 of the Companies Act, 2013.

CLAUSE (iv) COMPLIANCE WITH PROVISIONS OF SECTION 185 & 186

In respect of loans, investments, guarantees, and security, whether provisions of sections 185 and 186 of the Companies Act have been complied with, if not, provide the details thereof.

CLAUSE (v) DETAILS OF DEPOSITS

In respect of deposits accepted by the company or amounts which are deemed to be deposits, whether the directives issued by the Reserve Bank of India and the provisions of sections 73 to 76 or any other relevant provisions of the Companies Act and the rules made thereunder, where applicable, have been complied with, if not, the nature of such contraventions be stated; if an order has been passed by Company Law Board or National Company Law Tribunal or Reserve Bank of India or any court or any other tribunal, whether the same has been complied with or not.

CLAUSE (vi) COST RECORDS

Whether maintenance of cost records has been specified by the Central Government under subsection (1) of section 148 of the Companies Act and whether such accounts and records have been so made and maintained.

CLAUSE (vii) STATUTORY DUES

a) whether the company is regular in depositing undisputed statutory dues including Goods and Services Tax, provident fund, employees' state insurance, income-tax, sales-tax, service tax, duty of customs, duty of excise, value added tax, cess and any other statutory dues to the appropriate authorities and if not, the extent of the arrears of outstanding statutory dues as on the last day of the financial year concerned for a period of more than six months from the date they became payable, shall be indicated;

b) where statutory dues referred to in sub-clause (a) have not been deposited on account of any dispute, then the amounts involved and the forum where dispute is pending shall be mentioned (a mere representation to the concerned Department shall not be treated as a dispute).

CLAUSE (viii) DISCLOSURE OF UNRECORDED INCOME

Whether any transactions not recorded in the books of account have been surrendered or disclosed as income during the year in the tax assessments under the Income Tax Act, 1961, if so, whether the previously unrecorded income has been properly recorded in the books of account during the year.

CLAUSE (ix) DEFAULTS IN REPAYMENTS

a) whether the company has defaulted in repayment of loans or other borrowings or in the payment of interest thereon to any lender, if yes, the period and the amount of default to be reported as per the format below:-

Nature of borrowing, including debt securities	***Name of lender****	***Amount not paid on due date***	***Whether Principal or Interest***	***No. of delays or unpaid***	***Remarks, if any***
	*Lender wise details to be provided in case of defaults to banks, Financial Institutions and Government				

b) whether the company is a declared wilful defaulter by any bank or financial institution or other lender;

c) whether term loans were applied for the purpose for which the loans were obtained; if not, the amount of loan so diverted and the purpose for which it is used may be reported;

d) whether funds raised on short term basis have been utilised for long term purposes, if yes, the nature and amount to be indicated;

e) whether the company has taken any funds from any entity or person on account of or to meet the obligations of its subsidiaries, associates or joint ventures, if so, details thereof with nature of such transactions and the amount in each case;

f) whether the company has raised loans during the year on the pledge of securities held in its subsidiaries, joint ventures or associate companies, if so, give details thereof and also report if the company has defaulted in repayment of such loans raised.

CLAUSE (x) MONEY RAISED THROUGH PUBLIC ISSUE OR OTHERS

a) whether moneys raised by way of initial public offer or further public offer (including debt instruments) during the year were applied for the purposes for which those are raised, if not, the details together with delays or default and subsequent rectification, if any, as may be applicable, be reported;

b) whether the company has made any preferential allotment or private placement of shares or convertible debentures (fully, partially or optionally convertible) during the year and if so, whether the requirements of section 42 and section 62 of the Companies Act, 2013 have been complied with and the funds raised have been used for the purposes for which the funds were raised, if not, provide details in respect of amount involved and nature of non-compliance.

CLAUSE (xi) REORTING OF FRAUD

a) whether any fraud by the company or any fraud on the company has been noticed or reported during the year, if yes, the nature and the amount involved is to be indicated;

b) whether any report under sub-section (12) of section 143 of the Companies Act has been filed by the auditors in Form ADT-4 as prescribed under rule 13 of Companies (Audit and Auditors) Rules, 2014 with the Central Government;

c) whether the auditor has considered whistle-blower complaints, if any, received during the year by the company.

CLAUSE (xii) COMPLIANCES BY NIDHI COMPANY

a) whether the Nidhi Company has complied with the Net Owned Funds to Deposits in the ratio of 1: 20 to meet out the liability;

b) whether the Nidhi Company is maintaining ten per cent. unencumbered term deposits as specified in the Nidhi Rules, 2014 to meet out the liability;

c) whether there has been any default in payment of interest on deposits or repayment thereof for any period and if so, the details thereof.

CLAUSE (xiii) COMPLIANCES WITH RELATED PARTY TRANSACTIONS

Whether all transactions with the related parties are in compliance with sections 177 and 188 of Companies Act where applicable and the details have been disclosed in the financial statements, etc., as required by the applicable accounting standards.

CLAUSE (xiv) REPORTING ABOUT INTERNAL AUDIT SYSTEM

a) whether the company has an internal audit system commensurate with the size and nature of its business;

b) whether the reports of the Internal Auditors for the period under audit were considered by the statutory auditor.

CLAUSE (xv) REPORTING FOR NON-CASH TRANSACTIONS

Whether the company has entered into any non-cash transactions with directors or persons connected with him and if so, whether the provisions of section 192 of Companies Act have been complied with.

CLAUSE (xvi) COMPLIANCES WITH RBI DIRECTIVES

a) whether the company is required to be registered under section 45-IA of the Reserve Bank of India Act, 1934 and if so, whether the registration has been obtained;

b) whether the company has conducted any Non-Banking Financial or Housing Finance activities without a valid Certificate of Registration (CoR) from the Reserve Bank of India as per the Reserve Bank of India Act, 1934;

c) whether the company is a Core Investment Company (CIC) as defined in the regulations made by the Reserve Bank of India, if so, whether it continues to fulfil the criteria of a CIC, and in case the company is an exempted or unregistered CIC, whether it continues to fulfil such criteria;

d) whether the Group has more than one CIC as part of the Group, if yes, indicate the number of CICs which are part of the Group.

CLAUSE (xvii) DETAILS OF CASH LOSSES

Whether the company has incurred cash losses in the financial year and in the immediately preceding financial year, if so, state the amount of cash losses.

CLAUSE (xviii) DETAILS OF RESIGNATION OF AUDITORS

Whether there has been any resignation of the statutory auditors during the year, if so, whether the auditor has taken into consideration the issues, objections or concerns raised by the outgoing auditors.

CLAUSE (xix) ECONOMIC VIABLITY

On the basis of the financial ratios, ageing and expected dates of realisation of financial assets and payment of financial liabilities, other information accompanying the financial statements, the auditor's knowledge of the Board of Directors and management plans, whether the auditor is of the opinion that no material uncertainty exists as on the date of the audit report that company is capable of meeting its liabilities existing at the date of balance sheet as and when they fall due within a period of one year from the balance sheet date.

CLAUSE (xx) COMPLIANCES OF CSR RELATED OBLIGATIONS

a) whether, in respect of other than ongoing projects, the company has transferred unspent amount to a Fund specified in Schedule VII to the Companies Act within a period of six months of the expiry of the financial year in compliance with second proviso to sub-section (5) of section 135 of the said Act;

b) whether any amount remaining unspent under sub-section (5) of section 135 of the Companies Act, pursuant to any ongoing project, has been transferred to special account in compliance with the provision of sub-section (6) of section 135 of the said Act.

CLAUSE (xxi) UNFAVOURABLE REMARK IN SUBSIDIARY/ASSOCIATES' STANDALONE CARO REPORT

Whether there have been any qualifications or adverse remarks by the respective auditors in the Companies (Auditor's Report) Order (CARO) reports of the companies included in the consolidated financial statements, if yes, indicate the details of the companies and the paragraph numbers of the CARO report containing the qualifications or adverse remarks.

LESSON ROUND-UP

- **Standard on Internal Audit "Reporting**" issued by the Internal Audit Standards Board of ICAI specifies that the internal auditor's report should contain a clear written expression of significant observations, suggestions/ recommendations based on the policies, risks, controls and transaction processing taken as a whole and management responses. The process of reporting flows from overall internal audit objectives, as specified in the appointment letter.
- Internal audit report should be compact and easy to read, understandable to a broad audience. Internal audit report should be drafted in such a manner that the readers are easily able to scan an audit finding and take a decision about the corrective steps to be taken.
- **"Reporting"** lays down that the internal auditor's report should ordinarily include certain basic elements.
- **An illustrative layout is given below:**
  a) Title;
  b) Addressee;
  c) Period of coverage of the Report;
  d) Report Distribution List;
  e) Opening or introductory paragraph;
  f) Objectives/Scope paragraph (describing the nature of an internal audit);
  g) Executive Summary, highlighting the key material issues, observations, control weaknesses and exceptions;
  h) Observations, findings and recommendations made by the internal auditor;
  i) Comments from the local management;
  j) Action Taken Report — Action taken/ not taken pursuant to the observations made in the previous internal audit reports;
  k) Date of the report;
  l) Place of signature; and
  m) Internal auditor's signature with Membership Number.
- **Companies (Auditor's Report) Order, 2020 (CARO 2020):** In order to bring more transparency & faith in Financials Statements of companies, the Ministry of Corporate Affairs introduced the new set of Companies (Auditor's Report) Order, 2020 (CARO 2020).

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

1. State the Objectives of Reporitng?
2. Who are the users of Internal Audit Report?
3. Illustrate with examples the scope paragraph in Internal Audit Reporting?
4. Is CARO, 2020 ('the Order') applicable to audit report of an OPC (One Person Company) for the financial year 2021-22?

5. Will an OPC have to satisfy any conditions such as paid-up capital limit or turnover limit or paid up capital plus reserves limit to qualify for exemption from CARO, 2020?
6. What if paid-up share capital of an OPC is Rs. 1.25 crores as on 31.03.2022 and its turnover figures as per profit and loss account for financial years 2018-19, 2019-20, 2020-21 and 2021-22 are as follows:

Financial Year	*Turnover (Rs. in crores)*
2018-19	1.6
2019-20	1.8
2020-21	2.9
2021-22	12.0

Will it be exempt from CARO, 2020 for the financial year 2021-22?

7. The paid-up share capital X Private Ltd. as on 31.03.2022 is Rs. 1.50 crores. The reserves and surplus as on that date is Rs. 30 lakhs. The turnover of X Private Ltd as per profit and loss account for financial years 2019-20, 2020-21 and 2021-22 are as follows:

Financial Year	*Turnover (Rs. in crores)*
2018-19	7
2019-20	12
2020-21	15

Will the company be exempt from CARO, 2020 for the financial year 2021-22?

8. If a private limited company's paid up share capital is Rs. 2 crores or less as at 31.03.2022 and its turnover for 2020-21 is Rs. 20 crores or less, will it be necessary to compute the aggregate of paid up capital and reserves limit of Rs. 1 crore, borrowings limit of Rs. 1 crore and total revenue limit of Rs. 10 crores for determining exemption from applicability of CARO, 2020? Assume that the company is neither a subsidiary nor a holding company of a public company.
9. Is CARO applicable to foreign companies?
10. Is CARO applicable to LLP?
11. Is CARO 2020 applicable to consolidated financial statements?

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's

- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

Emerging Issues and Challenges

Lesson 9

KEY CONCEPTS

■ Financial Accounting Risk ■ Funding Risk ■ Conflict of Interest

Learning Objectives

To understand:

- What is Financial Accounting & the risks involved in Financial Accounting?
- How Financial Accounting Risks can be avoided?
- What is Funding Risks? How it can be avoided?
- Why funding risk to be considered in internal audit?
- Various business related challenges while conducting internal audit
- Prons and Cons of In-house Internal Audit function
- Prons and Cons of Outsourcing of Internal Audit function
- Prons and Cons of Co-sourcing of audit assignment
- Various emerging areas to be looked in Internal Audit

Lesson Outline

- Financial Accounting and Funding Risks
- Business Related Challenges
- In-house vs Outsourcing Audit Assignments
- Emerging Issues
- Emerging areas getting into focus in Internal Audit
- Lesson Round-Up
- Test Yourself
- List of Further Readings

FINANCIAL ACCOUNTING AND FUNDING RISKS

Many businesses have to take risks when it comes to their finances. Whether it's investing in new projects or increasing production, there is always the potential for failure. But with the proper financial accounting and funding risk management techniques, one can minimise their risk and ensure the success of business.

Financial accounting and funding risk are two different topics, but they go hand in hand. Financial accounting is the process of recording and summarising financial information, while funding risk is the potential for losses due to inadequate or inappropriate funding. How financial accounts are managed can significantly influence the level of funding risk a company faces.

Poorly managed accounts can lead to insufficient funds, which in turn, can lead to cash flow problems and other financial issues. On the other hand, well-managed accounts enable companies to utilise their resources efficiently and effectively, minimising their exposure to funding risks. Let's explore different ways to manage financial accounting and funding risks. We will also look at how financial accounting and funding risk are related and how organisations should manage their finances to reduce risk exposure.

What is Financial Accounting?

Financial accounting is the process of recording, classifying, and summarising financial transactions to provide useful information in making business decisions. The three primary financial statements are the balance sheet, income statement, and cash flow statement. Financial accounting also includes preparing reports for taxation, regulatory compliance, and management decision-making.

The purpose of financial accounting is to provide information that is useful in making business decisions. The information provided by financial accounting can be used to make an investment, financing, and operational decisions. Financial accounting information is also used by government agencies to make policy decisions.

Financial accounting aims to create transparent and accurate financial statements that conform to generally accepted accounting principles (GAAP). Financial statements should be free from material misstatements and provide a true and fair view of a company's financial position and performance.

What are the risks of Financial Accounting?

There are several risks associated with financial accounting, which can be broadly categorised into two main types:

1. Financial risks; and
2. Funding risks.

Financial risks include the risk of errors or omissions in financial statements, the risk of fraud or misappropriation of assets, and the risk of non-compliance with laws and regulations.

Funding risks include the risk that sufficient funds will not be available to meet obligations when they fall due, the risk of losing access to funding sources, and the risk of incurring additional costs in order to raise additional funds.

Both types of risks can significantly impact an organisation's ability to continue operating and achieving its strategic objectives. Therefore, effective management of these risks is essential to ensure the long-term success of any organisation.

How can you avoid Financial Accounting Risks?

There are a few key ways through which one can avoid financial accounting risks:

1. **Understand the financial statements:** Review income statement, balance sheet, and cash flow

statement on a regular basis. This will help to identify any potential red flags or areas of concern on timely basis.

2. **Maintain strong internal controls:** Having strong internal controls in place will help to ensure that financial information is accurate and reliable. Testing and review of internal controls and identifying the gaps allows to have better and thorough understanding of the standard operating procedures. It also gives the insight on creating better strategies to protect organisation's reputation and financial risk.
3. **Work with a reputed accountant or financial advisor:** Getting expert advice can help to navigate through complex financial issues and make sound decisions for business.

What is Funding Risk?

When it comes to financial accounting, funding risk is the potential risk that an organisation may face when it comes to its ability to obtain funding from lenders or investors. This type of risk can arise due to several factors, including the overall health of the economy, interest rates, and the specific financial situation of the organisation in question.

For organisations that are dependent on external financing, funding risk can be a major concern. If an organisation is unable to obtain the necessary funding to keep operating, it could quickly find itself in financial trouble. As such, it's crucial for organisations to monitor their funding risk and take steps to mitigate it where possible.

There are a few different ways that organisations can manage their funding risk. One common approach is known as "risk hedging." This involves taking out loans or lines of credit from multiple lenders to diversify the sources of funding and reduce reliance on any one particular lender. Another approach is maintaining strong relationships with existing lenders and investors and keeping them updated on organisation's financial situation. Doing so will make more likely to have their continued support in times of need.

Funding risk is an essential consideration for any company that relies on external financing. By taking steps to hedge against this risk and maintaining strong relationships with lenders and investors, can help to protect business from financial difficulties down the road.

Why should funding risk be considered in an internal audit?

When it comes to financial accounting, organisations must take into account funding risk in the decision-making process. This type of risk can come from a variety of sources, including changes in interest rates, regulatory changes, and economic conditions. While funding risk is often out of an organisation's control, there are still ways to manage and mitigate it. Internal audit can play a vital role in identifying and evaluating funding risks, as well as in providing recommendations on how to best manage them. By considering funding risk in internal audit, organisations can make more informed decisions that can help protect their bottom line.

When it comes to financial accounting, there is always the potential for funding risk. This is because organisations rely on outside sources of funding, such as loans, lines of credit, and investors. If these funding sources dry up, it can significantly impact a company's ability to continue operating.

Internal audit teams should also consider funding risk when evaluating a company's financial statements. They should look at things like cash flow and liquidity to see if there are any red flags that could indicate a problem with funding in the future. If there are concerns, the internal audit team can work with management to develop a plan to mitigate the risk.

Funding risk is just one of many risks that internal audit teams need to be aware of. By considering all risks, they can provide valuable insights that help organisations make better decisions and avoid financial problems down the road.

How can avoid Funding Risks?

There are a number of ways to avoid funding risks when it comes to financial accounting. First, be sure to have a clear understanding of organisation's financial situation and goals. This will help to make informed decisions about how to allocate funds and where to invest. One way is to choose investment vehicles carefully. Make sure to understand the risks associated with each type of investment before commit any money.

Another way to avoid funding risks is to diversify investments. Don't put all of eggs in one basket, so to speak. By spreading money around, can minimise the risk of losing everything if one particular investment goes sour. Diversifying will help protect from market fluctuations and other risks.

Finally, stay informed about the latest developments in the world of finance and investing. The more you know, the better equipped you'll be to make smart decisions about where to put your money. And always be prepared for the worst-case scenario. Have a contingency plan in place in case something goes wrong. By being proactive and prepared, can help minimise the impact of potential risks.

Let's discuss the practical examples from the past:

Example 1:

The fall of the energy trading corporation Enron Corporation in 2001 is a relevant example of financial accounting and funding risk. Enron was once one of the world's largest energy companies and was highly regarded for its innovative and sophisticated accounting practices. However, in the late 1990s, Enron began to face financial difficulties due to its heavy investments in speculative energy trading and its risky use of off-balance-sheet financing.

Enron's financial statements during this period were highly complex and difficult to understand, making it difficult for investors and analysts to fully assess the company's financial health. In addition, Enron engaged in aggressive accounting practices that allowed it to book revenue from deals that had not yet been completed, leading to inflated earnings reports and a false sense of financial stability.

Enron's funding risks became apparent in 2001 when the company's credit rating was downgraded, and lenders began to demand more collateral for its debt. This triggered a downward spiral for Enron, as the company's stock price plummeted, and it was unable to secure new funding. In December 2001, Enron filed for bankruptcy, causing significant financial losses for its shareholders, employees, and creditors.

The collapse of Enron resulted in widespread public outcry and led to increased scrutiny of accounting practices and financial regulation. The incident also highlighted the importance of transparent and accurate financial reporting, as well as the risks associated with complex financing structures and off-balance-sheet transactions.

Example 2:

The bankruptcy of the German payment processing business Wirecard AG in 2020 is another illustration of financial accounting and funding risk.

Wirecard was once considered a rising star in the financial technology industry, providing electronic payment and risk management services to businesses worldwide. However, in 2019, a series of investigative reports by the Financial Times alleged that Wirecard had inflated its revenue and profits through fraudulent accounting practices.

Wirecard initially denied the allegations and launched an internal investigation, but in June 2020, the company admitted that €1.9 billion ($2.2 billion) was missing from its accounts. The revelation triggered a sharp decline in Wirecard's stock price and led to its eventual collapse.

The Wirecard scandal has raised questions about the reliability of financial reporting and auditing, as well as the effectiveness of regulatory oversight. It has also led to a broader discussion about the risks associated with investing in high-growth technology companies and the need for greater transparency and accountability in the financial sector.

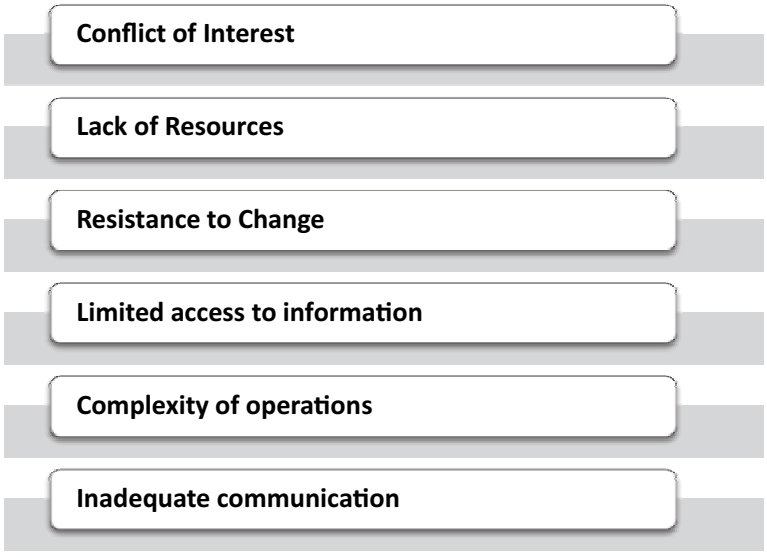
Conclusion

To summarise the discussion one can say, financial accounting and funding risk are two sides of the same coin. Poorly managed accounts can lead to insufficient funds, which in turn can lead to cash flow problems and other financial issues. On the other hand, well-managed financial statements help companies utilise their resources efficiently and effectively, minimising their exposure to risks.

Understanding the potential risks and taking steps to manage them properly can help ensure that business is financially successful. The use of financial accounting and funding risk can be complex and difficult to master, but the rewards for doing so are well worth it. Companies that understand the key concepts involved in these aspects of their business will have a much better chance of success than those that do not. Financial savvy is essential for businesses looking to survive in today's competitive economic environment, and having a firm understanding of financial accounting and funding risk can help give company that edge over the competition.

BUSINESS RELATED CHALLENGES

Conducting an internal audit of business can be a challenging task, and some of the common business-related challenges that may arise during the process include:



1. **Conflict of Interest:** One of the significant challenges of internal audit is managing the conflict of interest. In large business houses, Internal auditors are employees of the company, and they are expected to report on the operations of the business objectively. However, auditors may be hesitant to report negative findings if it could jeopardise their job security or relationship with their colleagues.

   For example, an auditor may face a conflict of interest if asked to audit the department where they worked before being appointed as an auditor. As a result, they may hesitate to report negative findings that could jeopardise their relationship with their former colleagues or impact their career prospects within the company.

Organisations can take the following precautions to avoid conflicts of interest in internal audit:

(i) **Develop and communicate clear policies:** Organisations should establish clear policies and procedures to identify and address potential conflicts of interest. These policies should outline the steps to be taken when conflicts arise, including recusal, disclosure, or seeking a second opinion.

(ii) **Ensure auditor independence:** Organisations should ensure that internal auditors have the necessary independence to conduct the audit objectively. This can be achieved by appointing auditors who are free from any conflicts of interest and establishing clear lines of reporting and accountability for auditors.

(iii) **Rotate auditors:** One way to reduce conflicts of interest is to rotate auditors between different departments or functions. This can help to reduce the risk of auditors becoming too close to the business units they are auditing and enhance the objectivity of the audit process.

(iv) **Encourage open communication:** Organisations should encourage open communication between auditors and management. This can help to ensure that any potential conflicts of interest are identified and addressed promptly.

(v) **Foster a culture of transparency:** A culture of transparency can help to reduce conflicts of interest by promoting openness and accountability. Organisations should establish clear channels for reporting conflicts of interest and provide support to auditors who raise concerns.

2. **Lack of resources:** Conducting an effective internal audit requires adequate resources, including skilled staff, technology, and time. However, many organisations may not allocate enough resources to an internal audit, resulting in suboptimal performance.

Lack of resources is a common challenge that organisations face when conducting internal audits. The lack of resources can compromise the quality and effectiveness of the audit process, leading to incomplete or inaccurate findings and recommendations.

To address the issue of lack of resources in internal audits, organisations can take the following steps:

(i) **Allocate sufficient resources:** Organisations should allocate adequate resources, including personnel, budget, and technology, to ensure that the internal audit team has the necessary support to conduct a thorough and effective audit.

(ii) **Prioritise audit activities:** Organisations should prioritise audit activities based on their impact and risk level. This can help to ensure that resources are allocated to the most critical areas, reducing the risk of overlooking critical issues.

(iii) **Adopt risk-based approach:** Adopting a risk-based approach to internal audit can help to focus the audit process on areas of highest risk. This approach can help to ensure that limited resources are used effectively and the audit team can provide more value to the business.

(iv) **Leverage technology:** Technology can help to enhance the efficiency and effectiveness of internal audits. Organisations should consider investing in technology tools, such as data analytics software, to help the audit team identify risks, analyse data, and automate manual processes.

(v) **Partner with external audit firms:** Organisations can also consider partnering with external audit firms to supplement their internal audit function. This can help to bring additional resources, expertise, and perspectives to the audit process, enhancing its effectiveness.

(vi) **Continuously review and adjust resource allocation:** Organisations should continuously review and adjust resource allocation to ensure that the audit function is adequately supported. Regular reviews can help to identify areas where additional resources are needed, and adjustments can help to ensure that the audit process remains effective and efficient.

3. **Resistance to change:** Internal audit may require changes in the business processes, systems, or culture. However, resistance to change may arise, making it difficult for the internal audit team to implement recommendations that could improve business operations.

   Resistance to change is a common challenge that organisations face when implementing new policies, procedures, or initiatives, including internal audits. Resistance to change can arise from a variety of factors, such as fear of the unknown, concerns about job security, and lack of trust in leadership. If not addressed effectively, resistance to change can hinder the success of internal audits and impede progress towards the organisation's objectives. To subdue resistance to change in internal audit, organisations can take the following steps:

   (i) **Communicate the need for change:** Organisations should communicate the need for change to all stakeholders and explain how the internal audit can help the organisation achieve its objectives. It is essential to be transparent about the reasons for the change and how it will benefit the organisation.

   (ii) **Involve stakeholders in the change process:** Involving stakeholders in the change process can help to address their concerns and build support for the internal audit. This can be achieved through consultation, collaboration, and active engagement with all affected parties.

   (iii) **Training and support:** Organisations should provide training and support to all stakeholders affected by the change, including the internal audit team, to help them understand their roles and responsibilities and build their capabilities. This can help to reduce anxiety and increase confidence in the new processes.

   (iv) **Recognise and address concerns:** Organisations should recognise and address any concerns or issues raised by stakeholders. This can be achieved through active listening, empathy, and problem-solving. It is important to acknowledge the validity of concerns and work with stakeholders to find solutions that meet their needs.

   (v) **Provide incentives:** Providing incentives, such as rewards, recognition, or promotions, can help to motivate stakeholders to embrace the change and support the internal audit. Incentives can also help to create a positive culture of change and reinforce the organisation's commitment to achieving its objectives.

   (vi) **Monitor and evaluate progress:** Organisations should monitor and evaluate the progress of the internal audit and the change process regularly. This can help to identify areas of success and areas for improvement and adjust the approach accordingly.

4. **Limited access to information:** Auditors require access to all relevant information to conduct a comprehensive internal audit. However, some business units may be reluctant to provide information, leading to gaps in the audit process.

   While performing internal audits, organisations frequently confront the problem of limited access to information. Limited access to information can arise due to a lack of data, insufficient system integration, or limited access to certain areas of the organisation. This challenge can compromise the quality and effectiveness of the audit process, leading to incomplete or inaccurate findings and recommendations. To conquer the issue of limited access to information in internal audits, organisations can take the following steps:

   (i) **Identify data sources:** Organisations should identify all possible data sources and determine which data is needed for the internal audit. This can include data from various systems, such as accounting systems, HR systems, and operational systems.

(ii) **Develop a data management plan:** Organisations should develop a data management plan that outlines how the data will be collected, stored, analysed, and shared. The plan should also include procedures for securing sensitive data and complying with regulatory requirements.

(iii) **Implement technology solutions:** Technology solutions, such as data analytics software and process automation tools, can help to streamline the data collection and analysis process. These solutions can also provide real-time insights into the organisation's operations, reducing the need for manual data collection.

(iv) **Establish data-sharing agreements:** Organisations should establish data-sharing agreements with relevant stakeholders, such as vendors, partners, and other organisations, to ensure access to necessary data. These agreements should include clear guidelines for data use, sharing, and security.

(v) **Develop a data governance framework:** Organisations should develop a data governance framework that defines the rules and processes for managing data throughout the organisation. The framework should include policies for data quality, security, privacy, and compliance.

(vi) **Train staff on data management:** Organisations should train their staff on data management practices, including data security, privacy, and quality. This can help to ensure that all employees are aware of their responsibilities and can contribute to the success of the internal audit.

5. **Complexity of operations:** Modern business operations are becoming increasingly complex, particularly in large and diversified organizations, which may make it difficult for internal auditors to understand the entire process or identify potential risks. It arises due to the multitude of processes, systems, and business units within an organisation, making it difficult to understand how they all fit together and how they impact the organisation's objectives. This can compromise the quality and effectiveness of the internal audit process, leading to incomplete or inaccurate findings and recommendations. To overcome this challenge in internal audits, organisations can take the following steps:

(i) **Conduct a process mapping exercise:** Organisations should conduct a process mapping exercise to identify all processes within the organisation and understand how they fit together. This can help to identify redundancies and inefficiencies and streamline processes to improve the effectiveness and efficiency of the organisation.

(ii) **Develop a risk assessment plan:** Organisations should develop a risk assessment plan that identifies potential risks associated with each process, system, and business unit. This can help prioritise the areas requiring the most attention and resources during the internal audit process.

(iii) **Establish clear objectives and criteria:** Organisations should establish clear objectives and criteria for the internal audit process. This can help to ensure that the audit team focuses on the areas that are most critical to the organisation's success and measures the effectiveness of the processes against the established criteria.

(iv) **Use data analytics and automation:** Data analytics and automation tools can help to streamline the internal audit process, reducing the time and effort required to analyze complex data sets. These tools can also provide real-time insights into the organisation's operations, enabling the audit team to identify patterns and trends quickly.

(v) **Involve relevant stakeholders:** Organisations should involve relevant stakeholders, such as process owners, system administrators, and business unit leaders, in the internal audit process. This can help to ensure that the audit team has access to the necessary information and can obtain an exhaustive understanding of the organisation's operations.

(vi) **Develop a comprehensive report:** Organisations should develop a comprehensive report summarising the findings and recommendations of the internal audit. The report should be clear and concise, highlighting areas of concern and providing actionable recommendations to address them.

6. **Inadequate communication:** Effective communication is critical for a successful internal audit. However, poor communication can lead to misunderstandings or misinterpretations of audit findings, ultimately undermining the effectiveness of the audit process.

   Inadequate communication can be a significant challenge for organisations conducting internal audits, particularly when different stakeholders have different levels of understanding about the audit process, objectives, and outcomes. Inadequate communication can result in misunderstandings, conflicts, and, ultimately, a lack of trust in the audit process. Organisations can take the following steps to overcome the challenge of inadequate communication in internal audits:

   (i) **Develop a communication plan:** Organisations should develop a communication plan outlining the key messages, audience, and communication channels throughout the audit process. The plan should also identify the stakeholders who need to be kept informed and how frequently they need to be updated.

   (ii) **Establish clear lines of communication:** Organisations should establish clear lines of communication with stakeholders throughout the audit process. This can include regular check-ins, progress reports, and feedback sessions.

   (iii) **Use clear and concise language:** Organisations should use clear and concise language in all communications related to the audit process. This ensures all stakeholders understand the audit process, objectives, and outcomes.

   (iv) **Address stakeholders' concerns:** Organisations should address stakeholders' concerns and questions throughout the audit process. This helps building trust and ensure stakeholders are engaged and invested in the process.

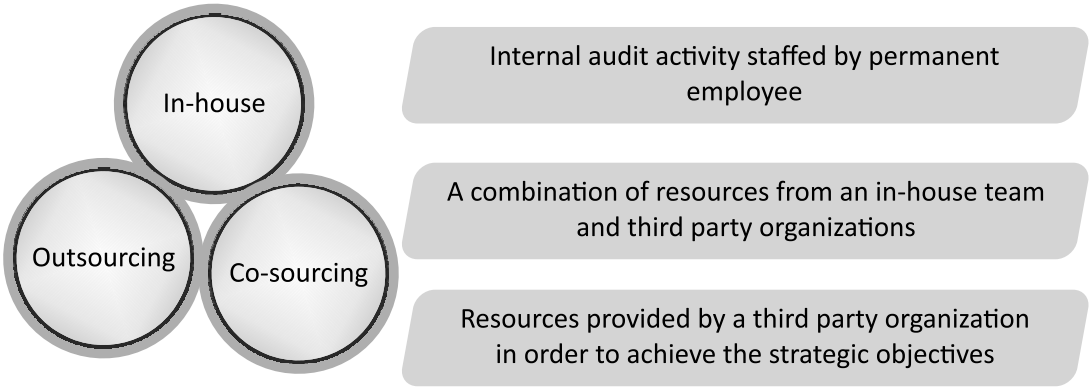
   (v) **Use visual aids:** Visual aids, such as graphs, charts, and diagrams, can help to communicate complex information in a more accessible way. This can help stakeholders to better understand the audit process and outcomes.

   (vi) **Foster an open and collaborative culture:** Organisations should foster an open and collaborative culture that encourages feedback and input from all stakeholders. This ensures that all perspectives are considered in the audit process, and that stakeholders feel valued and invested in the outcome.

IN-HOUSE VS. OUTSOURCING AUDIT ASSIGNMENTS

Internal audit assignments can be conducted either in-house or outsourced to external service providers. Both options have their own advantages and disadvantages, and the decision of whether to use in-house or outsourcing can vary depending on various factors, such as the size and complexity of the organisation, the availability of internal resources, and the cost and quality of external service providers.

Co-sourcing of audit assignments is an approach where an organisation combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organisations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing.



Pic 1: In-house vs. Outsourcing vs. Co-sourcing Internal Audit Assignments

In-house Function

Whether the organization choose to have internal audit as in-house function or otherwise, every choice has a pros and cons. Let's discuss the pros and cons of each option one by one:

Pros	***Cons***
✓ Continuity of Staff ✓ Certain controllable cost ✓ Full control of function ✓ A resource pool for the business ✓ Training ground for employees ✓ Greater cultural alignment ✓ Insiders	× May not be fully employed effectively and efficiently × Difficult to acquire necessary /maintain all skills and experience to meet the risk profile of the business × Need to continually invest in training and development × Recruitment hassles × Ineffective/inefficient start-up × Retention and development strategies required × Reduces opportunities to provide fresh perspective/risk of complacency or familiarity

Every industry is peculiar in nature, it has different ways of functioning and has different nuances. For example, in a pharmaceutical company, you need people that can understand research, manufacturing, design and selling. You need people that understand the underlying business and its risks, and also you need people who are experts in risk, risk management controls and processes.

Organisations can conduct internal audits themselves, but only when the auditor has the qualifications, competency and independence from the management structure to act with objectivity.

In an ideal situation, the organisation might employ someone with an accounting or other business degree; his or her skill set and professional demeanour might dovetail with those required to conduct comprehensive, independent internal audits. Alternatively, an employee may have sufficient cumulative industry experience, background and training to conduct internal audits. The knowledge an in-house internal auditor can acquire about the workings of the organisation can be a great benefit, and if he or she has longevity with the organisation, the historical perspective can be invaluable.

For example, Indian Oil Corporation Limited (IOCL) has a dedicated internal audit department that conducts audits across its various business units, including refining, marketing, and petrochemicals. The internal audit team is responsible for identifying risks, reviewing internal controls, and recommending improvements.

Outsourcing of Internal Audit Function

Should the organization perform internal audit function in-house or outsource it to a firm – which one is the better option? Either model can succeed or fail, but one will offer significant advantages depending on your needs and how you structure the function. Let's discuss the advantages and disadvantages of Outsourcing of the internal audit function:

Pros	***Cons***
✓ Established methodologies and benefits of refreshment based on experiences across different organisations ✓ Up-to-date skilled staff ✓ Ability to draw on a wide range of skills as and when required ✓ No time is taken up by managing service and resources ✓ Clearly defined service level and performance measures ✓ Easily established and quickly effective ✓ Credibility to third parties	× No permanent on-site resource to help other areas of the business × Potential cost impact × Possible lack of staff continuity × Remote from business developments, the culture and politics × Management time to establish and maintain relationships

Why outsourcing is a big risk?

Although outsourcing may seem attractive in theory, there are certain issues with internal capabilities that cannot be resolved, making it advantageous to keep internal audit in-house. The primary reason for outsourcing is to provide audit teams with access to a wide range of technical skills. However, many organizations have attempted to outsource engagements and failed to meet their objectives, prompting them to bring the work back in-house after just a few years.

Outsourcing and in-house approaches to IA each have their own advantages and challenges. Organizations with an in-house IA function are able to maintain complete control over their IA approach and have immediate knowledge of the issues at hand. However, since independence is a critical component of IA, careful consideration is required for the structure and reporting line of an in-house IA function.

Fully outsourcing of internal audit function can provide access to valuable expertise, cost flexibility, and an independent viewpoint that employees may not possess. It can also provide third-party assurance, as well as fresh industry or global perspectives. However, there may be a lack of internal knowledge, or it may take longer to grasp processes.

For example, Tata Steel recently outsourced its internal audit function to Ernst & Young in an effort to improve the efficiency and effectiveness of its internal audit processes. The external service provider is responsible for conducting internal audits across Tata Steel's various business units, including steel production, marketing, and sales.

Co-Sourcing of Audit Assignment

Co-sourcing of audit assignments is an approach where an organization combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organizations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing. Let's understand the advantages and disadvantages of the co-sourcing:

Pros	***Cons***
✓ Long-term permanent onsite presence through Head of Internal Audit ✓ Access to broad range of skills through the partner ✓ Draw on specialist skills as and when, and only when, needed ✓ Continuity through Head of Internal Audit ✓ Pull in up-to-date skills and experience as needed ✓ Quick to implement skills transfer to in-house team ✓ Flexible approach, clearly defined service level and KPI measures ✓ Credibility to third parties ✓ No or reduced training cost	× Time taken to recruit Head of Internal Audit × Possible cost impact × Management resource needed in recruitment and relationship development × Dependency of third part × Possible lack of staff continuity × Other challenges for in-house resources as discussed earlier

Co-sourcing can be particularly beneficial if the organisation has a continued relationship with the external IA supplier, so they can grow to understand the business. Co-sourcing can enable an organisation to top up skill sets, fill staff shortages, or perform work in various locations. An organisation could gain access to innovation in tools, audit techniques, thought leadership and benchmarking.

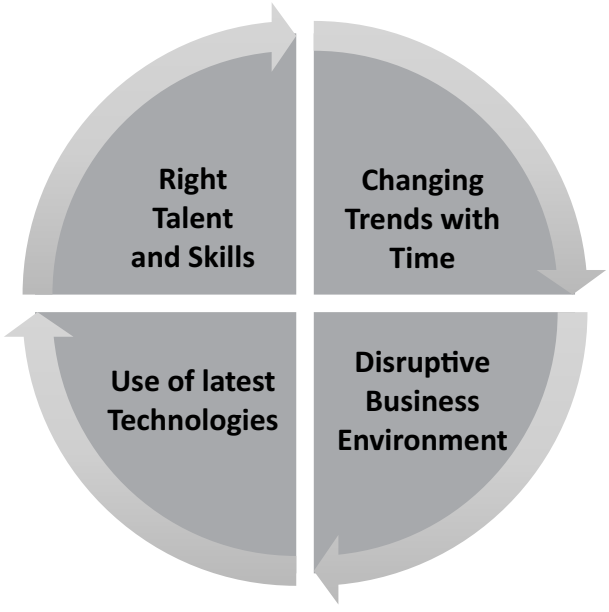
To successfully co-source audit assignments, it is important for the organization to establish clear communication channels, expectations, and roles and responsibilities for both in-house staff and external service providers. The organization should also have a clear understanding of the external service provider's qualifications, experience, and approach to auditing and should work with the provider to ensure that the audit process aligns with the organization's objectives and culture.

The challenges with co-sourcing can include the potential for confusion about responsibility and accountability and a lack of cultural fit if the external provider isn't aligned. Whatever combination of IA is settled upon, it must be judged according to whether it satisfies the expectations of stakeholders. It must demonstrate an awareness of the processes of the business and the risks it faces.

For example, the Indian Railway Catering and Tourism Corporation (IRCTC) recently implemented a co-sourcing model for its internal audit function, working with both in-house and external auditors to ensure that its audit function is aligned with its strategic objectives. The co-sourcing model allows IRCTC to access specialized expertise and gain external perspectives while maintaining control over the audit process.

The choice of in-house, outsourcing, or co-sourcing for internal audit assignments in India depends on the organization's size, complexity, and resources, as well as the availability of external service providers with the necessary expertise and experience. Each choice has its own advantages and disadvantages, and organizations should carefully consider their specific needs and objectives before making a decision.

EMERGING ISSUES



1. Changing Trends with Time

The field of internal audit is constantly evolving, and changing trends and times have a significant impact on how internal audits are conducted in the future. Here are some ways in which changing trends and times are likely to impact internal audit in the times to come:

(i) **Increased use of data analytics:** With the increasing amount of data being generated by organizations, internal auditors are expected to use data analytics tools to analyze and interpret data. This will require auditors to have a solid understanding of data analytics and data visualization tools and use them to provide insights and recommendations to management.

(ii) **Focus on risk management:** Internal auditors will be expected to focus more on risk management, including identifying and assessing risks, developing risk management strategies, and monitoring risk mitigation efforts. This will require auditors to have a deep understanding of the business and its risk profile.

(iii) **Emphasis on soft skills:** Internal auditors will be expected to have strong communication, critical thinking, and problem-solving skills. These skills will be crucial in effectively communicating audit findings to management and in collaborating with other departments and stakeholders.

(iv) **Impact of technology:** Technology is constantly changing, and internal auditors will be expected to keep up with the latest developments. This will require auditors to have an understanding of emerging technologies such as blockchain, artificial intelligence, and cybersecurity.

(v) **Increased focus on sustainability:** There is growing pressure on organizations to be more sustainable, and this will impact how internal audits are conducted. Auditors will be expected to assess the organization's sustainability practices and provide recommendations for improvement.

(vi) **Remote working:** With the pandemic, many organizations have shifted to remote working. This has created new challenges for internal auditors, who will need to adapt to conducting audits remotely, including using technology to conduct interviews, review documents, and communicate findings.

In summary, changing trends and times will continue to impact the field of internal audit in the times to come. Internal auditors will need to stay up-to-date with the latest trends and developments and be prepared to adapt their approach to effectively meet the changing needs of their organizations.

2. Disruptive Business Environment

Disruptive business environments can become an emerging issue in internal audit because they often create new risks and challenges for organizations that need to be addressed. These environments can be caused by a variety of factors, including technological innovations, changes in market conditions, regulatory changes, and other external factors.

As organizations adapt to these disruptive environments, they may need to change their business models, adopt new technologies, and revise their processes and procedures. This can create new risks, such as cybersecurity threats, compliance issues, and operational challenges. Internal auditors need to be aware of these risks and challenges and be prepared to assess and manage them.

In addition, disruptive environments can also create new opportunities for organizations, such as entering new markets or developing new products and services. Internal auditors need to be able to identify and evaluate these opportunities to ensure that they are pursued in a way that is consistent with the organization's strategy and objectives.

Overall, internal auditors need to be flexible, innovative, and adaptive in order to effectively address the risks and opportunities created by disruptive business environments. They need to have a deep understanding of the organization's operations and strategy, as well as the external factors that are driving change in the business environment. By doing so, they can provide valuable insights and assurance to the organization's stakeholders, including management, the board of directors, and external auditors.

A real-life example of a disruptive business environment that has become an emerging issue in internal audit is the rise of digital transformation. With the increased adoption of technology and the growth of digital platforms, many organizations are facing new risks and challenges related to cybersecurity, data privacy, and regulatory compliance.

For example, financial institutions are now required to comply with new regulations related to cybersecurity and data privacy, such as the General Data Protection Regulation (GDPR) in the European Union. These regulations require organizations to implement robust cybersecurity and data protection measures to safeguard customer information, which can be a significant challenge for organizations that are still using outdated technology or have limited resources for cybersecurity.

As a result, internal auditors in financial institutions need to be well-versed in the latest cybersecurity and data protection best practices and have the ability to assess and manage the risks associated with digital transformation. They may need to develop new audit procedures, such as reviewing the effectiveness of security controls for cloud-based systems or assessing the organization's ability to detect and respond to cyber threats in real-time.

In addition, the rise of digital platforms has also created new opportunities for financial institutions to innovate and create new products and services, such as mobile banking and online investment platforms. Internal auditors need to be able to identify and evaluate these opportunities and ensure that they are pursued in a way that is consistent with the organization's strategy and objectives.

3. Use of latest technologies

The use of latest technologies in systems in organizations is an emerging issue in internal audit, as it presents new risks and challenges that internal audit must address. Here are some areas that internal audit should focus on when auditing the use of latest technologies in systems:

(i) **Security and Privacy:** With the use of latest technologies, there is an increased risk of cyber threats and data breaches. Internal audit should ensure that the systems are secure and that appropriate measures are in place to protect sensitive data. This includes an assessment of the security protocols, encryption, access controls, and other security measures.

(ii) **Governance and Management:** Internal audit should review the governance structure in place to ensure that there are adequate controls and oversight of the technology initiatives. This should include an assessment of the roles and responsibilities of key stakeholders, including the board, senior management, and the IT team. Additionally, internal audit should review the policies and procedures in place to ensure that they are adequate and up to date.

(iii) **System Development Life Cycle:** Internal audit should ensure that appropriate controls are in place throughout the system development life cycle, from design to implementation to maintenance. This includes an assessment of the testing and validation procedures, as well as the change management process.

(iv) **Business Continuity and Disaster Recovery:** Internal audit should ensure that appropriate measures are in place to ensure business continuity in the event of a system outage or disaster. This includes an assessment of the backup and recovery procedures, as well as the disaster recovery plan.

(v) **Compliance:** Internal audit should ensure that the use of latest technologies is compliant with applicable laws and regulations. This includes an assessment of the data protection laws, industry-specific regulations, and other compliance requirements.

In summary, internal audit should focus on security and privacy, governance and management, system development life cycle, business continuity and disaster recovery, and compliance when auditing the use of latest technologies in systems. By doing so, internal audit can help to ensure that the risks associated with the use of these technologies are effectively managed and that the organization is able to leverage the benefits of these emerging technologies.

Sure, here's a real-life case study from India on the use of latest technologies in systems and the associated risks that internal audit must address.

In recent years, many Indian organizations have started using biometric authentication technology for employee attendance tracking and access control. Biometric authentication involves the use of unique biological characteristics, such as fingerprints or facial recognition, to verify the identity of an individual.

While biometric authentication can provide organizations with many benefits, such as increased accuracy, reduced fraud, and improved security, it also presents new risks that internal audit must address. Here are some examples:

Privacy: Biometric authentication involves the collection and processing of sensitive personal data, such as fingerprints or facial recognition data. Internal audit must ensure that appropriate privacy controls are in place, such as obtaining consent from employees, limiting access to the data, and encrypting the data to protect the privacy of personal data.

Security: Biometric authentication can be vulnerable to hacking, spoofing, or other attacks, which can compromise the security of the organization's systems and data. Internal audit must ensure that appropriate security controls are in place, such as implementing multi-factor authentication, using secure encryption algorithms, and conducting regular vulnerability assessments to protect the organization's systems and data.

Compliance: Biometric authentication is subject to data protection and privacy regulations, such as the Personal Data Protection Bill, 2019, and the Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Data or Information) Rules, 2011. Internal audit must ensure that the organization's use of biometric authentication complies with these regulations and that appropriate controls are in place to protect the privacy of personal data.

For example, a leading Indian IT services company implemented a biometric authentication system for employee attendance tracking and access control at its offices. The system was based on facial recognition technology, which involved capturing and storing images of employees' faces for authentication purposes.

To address the risks associated with biometric authentication, the company's internal audit team conducted a review of the system, including an assessment of the privacy, security, and compliance controls. The audit team identified several areas for improvement, such as enhancing the security controls, improving the data retention policies, and conducting regular privacy impact assessments.

Based on the audit findings, the company implemented several changes to the biometric authentication system, such as using better encryption algorithms, limiting the retention of facial recognition data, and obtaining employee consent for the use of biometric authentication. These changes helped the company to manage the risks associated with biometric authentication and to ensure compliance with data protection regulations.

4. Right Talent and Skills

The rapid pace of technological advancement and constantly evolving business models and processes have led to an increased demand for specialised skills in various fields. This is particularly true for the internal audit function, which must keep up with changing trends and technologies in order to effectively identify and mitigate risks within an organisation.

The right talent with the appropriate skills and knowledge is critical for internal audit to be effective in the current business environment. For example, as companies adopt new technologies such as artificial intelligence, the internal audit function must have the skills and expertise to evaluate the effectiveness of these tools and their impact on the organization's risk profile.

Additionally, the increasing importance of data analytics in internal audit means that the function requires talent with skills in data science, statistical analysis, and visualization. Internal auditors must also have a strong understanding of cybersecurity and be able to identify and mitigate potential security risks.

The emerging issue in conducting internal audit is the challenge of finding and retaining talent with the necessary skills and expertise to meet the changing demands of the function. As companies compete for talent in these specialized fields, it can be difficult for internal audit functions to attract and retain top talent.

To address this challenge, organizations may need to invest in training and development programs to help internal auditors acquire the necessary skills and expertise. They may also need to consider alternative talent models, such as partnering with external service providers or leveraging the gig economy to tap into specialized talent on an as-needed basis.

Example: Let's say that a manufacturing company is implementing a new robotic process automation (RPA) system to automate certain tasks in their production line. As part of the implementation process, the internal audit function is tasked with evaluating the effectiveness of the RPA system and identifying any potential risks associated with its use.

To conduct this evaluation, the internal audit team needs to have talent with knowledge and skills in RPA technology, as well as an understanding of the manufacturing processes and associated risks. The team may also need to have experience in evaluating the effectiveness of similar technology systems in other companies.

If the internal audit function does not have the necessary talent with the required skills and expertise, they may struggle to effectively evaluate the RPA system and identify any risks. This could result in the company unknowingly exposing itself to potential risks associated with the use of the technology.

On the other hand, if the internal audit function has the right talent with the appropriate skills, they can provide valuable insights and recommendations to help the company effectively manage risks associated with the RPA system. This highlights the importance of having the right talent with changing pace and trends in internal audit to ensure the function can effectively identify and mitigate risks.

In recent years, the financial services industry has seen a rapid transformation driven by digital disruption and regulatory changes. This has led to a growing demand for specialized skills in areas such as cybersecurity, data analytics, and emerging technologies like blockchain and artificial intelligence.

To keep up with these changes and effectively manage risks, internal audit functions in financial services organizations have had to adapt and evolve. For example, they are increasingly leveraging data analytics to identify potential fraud and other risks, as well as using artificial intelligence to enhance the efficiency and effectiveness of audits.

However, finding and retaining talent with the necessary skills and expertise can be a challenge for these organizations. This is especially true as competition for talent in these areas is high, with technology companies and other industries also competing for these specialized skills.

One way that financial services organizations are addressing this challenge is by investing in training and development programs to upskill their existing staff. They are also exploring alternative talent models, such as partnering with external service providers or leveraging the gig economy to access specialized talent on an as-needed basis.

Overall, this example highlights how talent with changing pace and trends is impacting the internal audit function in financial services organizations, and the need for these organizations to be proactive in addressing this challenge in order to effectively manage risks and ensure compliance with regulatory requirements.

EMERGING AREAS GETTING INTO FOCUS IN INTERNAL AUDIT

Internal audit is a constantly evolving field, with new areas of focus emerging as organisations and industries change. Some emerging areas getting into focus in internal audit include:

1. **Cybersecurity:** With the increasing reliance on technology and the rise of cyber threats, internal auditors are increasingly being called upon to assess and monitor the effectiveness of an organization's cybersecurity measures.

Example 1:

Let's discuss the case of Bank of Baroda, where internal audit played a significant role in cyber security is the 2016 cyber attack. In this incident, hackers managed to steal approximately $13.5 million from the bank by hacking into the bank's SWIFT messaging system.

Following the incident, the bank's internal audit function conducted a comprehensive review of the bank's cyber security policies and procedures. The review identified several weaknesses in the bank's cyber security controls, including a lack of employee awareness and training on cyber security, inadequate incident response procedures, and outdated software systems.

The internal audit team made several recommendations to improve the bank's cyber security posture. These included increasing employee awareness and training on cyber security, implementing stronger access controls, and upgrading the bank's software systems.

The bank implemented these recommendations and took several additional steps to improve its cyber security. These included hiring a chief information security officer, establishing a dedicated cyber security operations center, and implementing a robust incident response plan.

As a result of these measures, the Bank of Baroda was able to strengthen its cyber security posture and prevent further cyber attacks. The incident highlights the critical role of internal audit in identifying and mitigating cyber security risks and the importance of continuous improvement in cyber security policies and procedures.

Example 2:

Another example where internal audit played a significant role in cyber security is the 2020 cyber-attack on Dr. Reddy's Laboratories, one of India's largest pharmaceutical companies.

In October 2020, Dr. Reddy's Laboratories was hit by a cyber attack that impacted its global operations. The attack disrupted the company's manufacturing, research, and development operations, and led to a temporary shutdown of some of its plants.

The company's internal audit function played a critical role in responding to the attack and mitigating its impact. The internal audit team worked closely with the company's IT department to assess the scope and severity of the attack, identify vulnerabilities in the company's cyber security controls, and develop a plan to mitigate the impact of the attack.

The internal audit team identified that the cyber attackers used a phishing email to gain access to the company's systems. They also found that the company's network segmentation was inadequate, which allowed the attackers to move laterally across the company's network and infect multiple systems.

The internal audit team made several recommendations to improve the company's cyber security posture, including the implementation of multi-factor authentication for all employees, improving network segmentation, and increasing employee awareness and training on cyber security risks.

The company implemented these recommendations and took several additional steps to strengthen its cyber security posture. These included increasing its investment in cyber security technologies and tools, hiring additional cyber security personnel, and conducting regular vulnerability assessments and penetration testing.

As a result of these measures, Dr. Reddy's Laboratories was able to recover from the cyber attack and resume its operations. The incident highlights the critical role of internal audit in identifying and mitigating cyber security risks, and the importance of continuous improvement in cyber security policies and procedures to protect against cyber threats.

2. **ESG (Environmental, Social, and Governance):** As environmental, social, and Governance risks are becoming a major concern for organisations, internal auditors are being asked to assess the company's performance in these areas and help to identify potential risks.

Example:

Tata Group is one of the example of ESG from an internal audit perspective. The Tata Group is a multinational conglomerate based in India with interests in various industries including steel, automobiles, and information technology.

The Tata Group has been committed to sustainability and ESG for several years and has made significant efforts to integrate ESG considerations into its business operations. In 2014, the company established a dedicated sustainability department to oversee and manage its ESG initiatives.

To ensure that its ESG efforts are aligned with its business strategy and goals, the Tata Group conducts regular internal audits of its sustainability practices. The internal audit team evaluates the company's ESG performance against various parameters, including resource efficiency, climate change, and social responsibility.

The internal audit team also conducts periodic assessments of the company's supply chain to identify potential ESG risks and opportunities. For example, the team assesses supplier's compliance with the company's code of conduct, which includes requirements related to labor standards, human rights, and environmental stewardship.

The internal audit team at Tata Group also works closely with other departments to identify and address ESG-related issues. For example, the team collaborates with the legal department to ensure compliance with applicable environmental and social regulations.

Through its ESG efforts, Tata Group has been able to improve its environmental performance and social impact, while also creating long-term value for its stakeholders. The company has been recognized for its sustainability leadership, including being ranked as the top Indian company in the Dow Jones Sustainability Index for several years in a row.

3. **Artificial Intelligence (AI):** The use of AI is increasing in various aspects of organisations, and internal auditors are being asked to assess the effectiveness of the controls put in place to manage the risks associated with AI.

Example:

One notable case study on the use of artificial intelligence in internal audit comes from Wipro Limited, a multinational IT services company headquartered in Bangalore.

Wipro Limited implemented an AI-based platform called Holmes, which is designed to help internal audit teams improve their efficiency and effectiveness. The platform uses machine learning algorithms to analyze large volumes of data from various sources, such as financial statements, invoices, and customer feedback.

Holmes can perform a variety of tasks, such as identifying patterns and anomalies in data, detecting potential fraud and errors, and generating reports with insights and recommendations. The platform can also learn from past audits to improve its accuracy and effectiveness over time.

Wipro Limited has reported significant benefits from using Holmes in its internal audit process. For example, the company has been able to reduce the time and effort required for audits by up to 30%, while also increasing the coverage and accuracy of its audits. The platform has also helped the company identify and mitigate potential risks more effectively, which has contributed to better overall business outcomes.

4. **Regulatory and Risk compliance:** With constantly evolving regulatory landscape, internal auditors are required to stay up-to-date with changes in regulations and help ensure that the organisation complies with them.

CASE STUDY

Volkswagen's Emissions Scandal

In 2015, the German automaker Volkswagen (VW) was found to have installed software in its diesel cars that could cheat emissions tests. The software, known as a "defeat device," was designed to detect when the car was being tested for emissions and to reduce the emissions to comply with regulations. However, in real-world driving, the cars emitted up to 40 times the legal limit of nitrogen oxide (NOx) emissions.

The scandal was a result of the company's non-compliance with emissions regulations, which led to serious legal, financial, and reputational consequences. VW was forced to recall millions of cars and pay billions of dollars in fines, settlements, and compensation to customers. The company also faced criminal charges and had to make significant changes to its corporate culture and Governance.

The scandal also had a ripple effect on the automotive industry as a whole, leading to increased scrutiny of emissions testing and regulatory compliance. It also raised questions about the role of regulators and their ability to detect and prevent similar violations in the future.

The VW scandal demonstrates the importance of regulatory and compliance risks in the automotive industry and beyond. Companies must ensure that their products and practices comply with regulations and standards, and they must be transparent and accountable to regulators and customers. Failure to do so can result in serious legal, financial, and reputational consequences, as well as harm to public health and the environment.

CASE STUDY

PNB's Fraudulent Transactions

In 2018, Punjab National Bank (PNB), one of the largest public sector banks in India, discovered a fraudulent transaction of approximately Rs. 14,000 crore ($1.8 billion) at its Brady House branch in Mumbai. The fraud involved the bank's employees colluding with companies owned by Nirav Modi, a billionaire jeweler, to obtain unauthorised loans and letters of credit.

The fraud was a result of the bank's non-compliance with banking regulations and internal controls, which allowed the employees to bypass the bank's systems and processes. The employees were able to issue unauthorised letters of credit to Modi's companies without collateral or guarantees, and the transactions went undetected for several years.

The fraud had serious legal, financial, and reputational consequences for the bank and its stakeholders. PNB's stock price and credit ratings fell, and the bank had to make provisions for the fraudulent transactions, which led to a significant loss. The fraud also raised questions about the effectiveness of the bank's internal controls and the role of regulators in detecting and preventing such frauds.

The PNB fraud highlights the importance of regulatory and compliance risks in the banking industry in India. Banks must comply with the regulatory requirements and ensure the effectiveness of their internal controls to prevent frauds and other financial crimes. The fraud also underscores the need for transparency and accountability in the banking sector and the importance of the role of regulators in enforcing regulations and protecting the interests of stakeholders.

5. **Supply chain risks:** The COVID-19 pandemic has highlighted the risks associated with global supply chains. Internal auditors are being asked to assess the organization's supply chain risks and help identify potential vulnerabilities.

Example 1:

A very good example on supply chain risk from an internal audit perspective is the 2019 Indian Auto Parts Manufacturer (APM) crisis. The APM company was a major supplier of auto parts to various automobile manufacturers, including some of the biggest names in the industry.

The crisis began when the company faced financial difficulties due to a severe cash crunch, which was caused by a combination of factors, including high debt levels, poor financial management, and delays in payments from customers. As a result, the company was unable to pay its suppliers for the raw materials required to manufacture auto parts.

This led to a cascading effect on the supply chain, with the company unable to meet its delivery commitments to its customers. The automobile manufacturers, in turn, faced production delays, which impacted their ability to meet their own delivery commitments to their customers. This led to a ripple effect on the entire supply chain, causing significant disruptions and losses for all parties involved.

This crisis highlighted the importance of assessing supply chain risks and ensuring the implementation of robust risk management processes. A key lesson learned from this crisis was the need for better financial management and transparency in the supply chain, including a focus on timely payment of suppliers and effective cash flow management.

The crisis also demonstrated the need for greater collaboration and communication across the supply chain, including regular monitoring of supplier performance and contingency planning to mitigate potential disruptions. This highlights the importance of regular internal audits and risk assessments to identify potential areas of weakness in the supply chain and to implement effective controls and contingency plans to minimize the impact of any potential disruptions.

Example 2:

Another example on supply chain risk is the 2020 COVID-19 pandemic and its impact on the pharmaceutical industry in India. The pandemic had a significant impact on the global supply chain, with disruptions in the transportation of goods, delays in customs clearance, and reduced availability of raw materials. These disruptions had a direct impact on the pharmaceutical industry, which relies heavily on imports of raw materials and intermediate products from China and other countries.

This crisis highlighted the importance of assessing and managing supply chain risks, including the need for contingency planning to address potential disruptions. The crisis also emphasised the need for greater collaboration and communication across the supply chain to mitigate the impact of any potential disruptions.

The pharmaceutical industry in India responded by implementing a range of measures to mitigate the impact of the pandemic on the supply chain, including increasing the inventory of critical raw materials, diversifying suppliers, and building strategic partnerships with local manufacturers. These measures helped to mitigate the impact of the pandemic on the pharmaceutical industry in India, ensuring the continuity of critical supplies and medicines.

The crisis also underscored the need for regular internal audits and risk assessments to identify potential areas of weakness in the supply chain and to implement effective controls and contingency plans to minimize the impact of any potential disruptions. In addition, it highlighted the importance of monitoring supplier performance, identifying potential risks, and building stronger partnerships with key suppliers to ensure the continuity of critical supplies.

6. **Data privacy:** As organisations collect more and more data, internal auditors are being asked to assess the effectiveness of the organization's data privacy controls and help identify potential risks.

Example:

The 2018 Cambridge Analytica scandal involving Facebook is a very good example of data privacy concerns. Cambridge Analytica was a political consulting firm that used data from millions of Facebook users without their consent to create targeted political ads and influence the 2016 US presidential election.

The scandal came to light after a whistleblower, Christopher Wylie, revealed that Cambridge Analytica had obtained data from an app developed by researcher Aleksandr Kogan. The app, called "This Is Your Digital Life," was a personality quiz that collected data on not only the users who took the quiz but also their friends on Facebook.

While Facebook's policies at the time allowed third-party developers to collect user data, they were not allowed to share that data without explicit user consent. It was later revealed that Cambridge Analytica had obtained data from 87 million Facebook users, most of whom had not given their consent for their data to be shared.

The scandal sparked widespread outrage and calls for greater data privacy protections. In response, Facebook made several changes to its policies and platform, including limiting third-party access to user data and implementing more stringent privacy controls.

The Cambridge Analytica scandal serves as a cautionary tale about the importance of protecting personal data and the potential consequences of failing to do so. It highlights the need for greater transparency and accountability in how companies collect, store, and use personal data, as well as the importance of giving users control over their own data.

CASE STUDY

Whatsapp

Another recent example of a data privacy concern is the 2021 WhatsApp privacy policy update controversy. WhatsApp is a popular messaging app used by millions of people in India and around the world. In January 2021, the company announced an updated privacy policy that would allow it to share certain user data with its parent company, Facebook.

The announcement sparked concerns among Indian users and led to widespread backlash, with many people expressing concerns about the potential misuse of their data. Some users began to migrate to alternative messaging apps such as Signal and Telegram, which have stricter privacy policies and do not share user data with third parties.

The Indian government also became involved in the controversy, with the Ministry of Electronics and Information Technology issuing a notice to WhatsApp asking the company to withdraw the updated privacy policy. The government expressed concerns that the policy violated the privacy of Indian users and was not in compliance with Indian laws.

WhatsApp initially defended the policy, claiming that it did not compromise the privacy of users and that the company was committed to protecting user data. However, in response to the backlash and government pressure, WhatsApp delayed the implementation of the policy and began a campaign to educate users about its privacy practices.

The WhatsApp privacy policy update controversy highlights the importance of transparency and user control in data privacy. It also underscores the need for companies to comply with local laws and regulations and to take the concerns of their users seriously. The incident has spurred discussions about data privacy in India and the need for stronger privacy protections for Indian users.

7. **Fraud prevention:** Fraud prevention is an important aspect of any organisation's risk management framework. Internal audit can play a crucial role in fraud prevention by identifying and assessing the risks of fraud, evaluating the effectiveness of existing controls, and recommending improvements to prevent and detect fraud.

   The internal audit team of the Indian subsidiary received an anonymous tip-off that an employee was colluding with a vendor to submit inflated invoices for goods and services that were never actually provided. The employee was working in the finance department and was responsible for processing vendor invoices and making payments to vendors.

   The internal audit team decided to investigate the tip-off and found that the employee had indeed colluded with the vendor to submit inflated invoices. The employee had created fictitious purchase orders and approved the invoices for payment without verifying the goods and services had been received. The vendor would then transfer a portion of the payments back to the employee as kickbacks.

Here's how the internal audit team helped to prevent the fraud from occurring:

- **Identifying Weaknesses in Controls:** The internal audit team found that there were several weaknesses in the control environment around the vendor invoice process, which had allowed the employee to collude with the vendor.
- **Recommending Controls Improvements:** The internal audit team recommended several control improvements to strengthen the vendor invoice process and prevent fraud in the future. The recommendations included segregation of duties, more stringent vendor onboarding procedures, and more rigorous verification of vendor invoices.
- **Preventing Further Losses:** The internal audit team's timely intervention and recommendations helped the company to prevent further losses and take corrective action against the employee and the vendor. The employee was terminated, and the vendor was blacklisted.

In short, the internal audit team's proactive approach and diligent investigation helped to prevent fraud from occurring by identifying weaknesses in controls and recommending improvements to prevent similar frauds in the future. This highlights the importance of internal audit's role in fraud prevention, not just detection, and the need for organizations to take a proactive approach to managing fraud risks.

8. **Social media:** Social media is a powerful tool for organisations, but it also presents new risks, such as reputational damage and cybersecurity threats. Internal auditors are being asked to assess the organization's social media strategy and help identify potential risks associated with social media use.

   Social media has had a significant impact on organizations, and internal auditors play a crucial role in assessing and managing the associated risks. Here are some perspectives on the impact of social media on organizations from an internal audit perspective:

   (i) **Reputational risk:** Social media has given organizations a powerful tool for communication and brand building. However, it has also exposed them to significant reputational risk. Negative comments, complaints, and criticism can spread rapidly and damage an organization's reputation. Internal auditors need to evaluate the organization's social media presence and ensure that appropriate controls and monitoring mechanisms are in place to manage this risk.

   (ii) **Information security risk:** Social media platforms collect and store a vast amount of personal and organizational information. This information can be used for cyber attacks, social engineering, and other security breaches. Internal auditors should evaluate the organization's social media policies and practices to ensure that information security risks are effectively managed.

   (iii) **Compliance risk:** Social media use is subject to numerous regulatory requirements, such as data privacy laws, advertising regulations, and social media guidelines. Internal auditors need to assess whether the organization's social media activities comply with these regulations and guidelines.

   (iv) **Employee productivity and conduct:** Social media can impact employee productivity and behavior. Internal auditors should evaluate the organization's policies and practices related to social media use by employees and ensure that they are consistent with the organization's values and culture.

   (v) **Business opportunities:** Social media can also provide new business opportunities, such as social media marketing and e-commerce. Internal auditors should evaluate the organization's social media strategy and assess the risks and benefits associated with social media use for business purposes.

By evaluating social media policies and practices and implementing appropriate controls, internal auditors can help organizations leverage the benefits of social media while minimizing the associated risks.

Example 1:

Aadhaar is a unique identification number issued by the Indian government, and it is linked to an individual's biometric and demographic data. In 2017, it was reported that the Aadhaar database had been breached, and personal data of millions of Indian citizens was leaked online.

This highlights the information security risks associated with social media use. The leaked data was reportedly being sold on social media platforms, raising concerns about how easily personal information could be accessed and misused. Internal auditors would have needed to evaluate the government's social media policies and practices to ensure that appropriate controls were in place to protect sensitive data.

This incident also underscores the compliance risk associated with social media use. Aadhaar is subject to numerous regulatory requirements, including data privacy laws and information security guidelines. Internal auditors would need to assess whether the government's social media activities related to Aadhaar were compliant with these regulations and guidelines.

In response to the incident, the Indian government took several measures, such as strengthening the security protocols for Aadhaar and establishing a dedicated authority for data protection. Internal auditors would also need to evaluate the effectiveness of these measures in managing the risks associated with social media use and information security.

Example 2:

In July 2020, it was reported that several high-profile Twitter accounts, including those of Barack Obama, Elon Musk, and Bill Gates, had been hacked, and a bitcoin scam was posted from these accounts.

This incident highlights the information security risks associated with social media use. The hackers reportedly gained access to Twitter's internal systems and tools, allowing them to take control of high-profile accounts and post the scam message. Internal auditors would have needed to evaluate Twitter's social media policies and practices to ensure that appropriate controls were in place to prevent unauthorized access to sensitive data and systems.

This incident also underscores the reputational risk associated with social media use. The hack received widespread media attention and caused significant damage to Twitter's reputation. Internal auditors would need to assess whether Twitter's incident response plan was adequate to manage the reputational risks associated with such incidents.

In response to the incident, Twitter made several changes to its security protocols and procedures, such as implementing two-factor authentication for all accounts and restricting access to internal tools. Internal auditors would also need to evaluate the effectiveness of these measures in managing the risks associated with social media use and information security.

9. Culture audit: Culture is an important factor in organisational success and can have a significant impact on risk management. Internal auditors are being asked to assess the culture of the organization and help identify potential cultural risks that may affect the organization's objectives.

Organisational culture can have a significant impact on the effectiveness of an organization's Governance, risk management, and control processes. Here are a few ways in which internal auditors can evaluate and assess organizational culture:

(i) Conduct culture assessments: Internal auditors can conduct culture assessments to gain insight into the organization's values, beliefs, and behaviors. This can involve conducting interviews, surveys, and focus groups with employees at all levels of the organization.

(ii) **Evaluate tone at the top:** Internal auditors can assess the tone at the top by evaluating the leadership's behavior and how it influences the organization's culture. Tone at the top can affect the behavior of employees, and therefore, has a significant impact on the effectiveness of risk management and control processes.

(iii) **Review policies and procedures:** Internal auditors can review policies and procedures to ensure that they are consistent with the organization's values and culture. Policies that are inconsistent with the organization's culture can lead to employees feeling disconnected from the organization's values and beliefs.

(iv) **Assess employee engagement:** Internal auditors can assess employee engagement to determine how engaged employees are with the organization's culture. Engaged employees are more likely to understand and follow the organization's values and beliefs, leading to a more effective risk management and control environment.

(v) **Evaluate training and communication:** Internal auditors can evaluate the organization's training and communication programs to determine how well they promote the organization's culture. Training and communication programs that are aligned with the organization's culture can help employees understand the importance of the organization's values and beliefs.

Example:

In 2018, the U.S. Olympic Committee (USOC) commissioned a culture audit in response to a sexual abuse scandal involving USA Gymnastics, one of its national governing bodies. The audit aimed to assess the organizational culture within the USOC and identify any systemic issues that may have contributed to the abuse scandal.

The culture audit involved conducting interviews with over 150 people, including current and former athletes, coaches, staff, and board members. The audit also included a review of policies and procedures, as well as an analysis of the organization's leadership and communication practices.

The audit identified several areas where the USOC's culture needed improvement, including:

- Lack of transparency: The audit found that there was a lack of transparency in the USOC's decision-making processes, which contributed to a lack of trust among athletes and other stakeholders.
- Inadequate communication: The audit found that there was a lack of clear and consistent communication within the USOC, which led to confusion and misunderstandings.
- Focus on winning at all costs: The audit found that the USOC's emphasis on winning medals sometimes overshadowed its commitment to athlete safety and well-being.

As a result of the audit, the USOC implemented several changes to its culture and Governance, including the establishment of an Athlete Ombudsman, increased funding for athlete safety and support programs, and the creation of a new Ethics and SafeSport Division.

This demonstrates how a culture audit can be a valuable tool for identifying and addressing systemic issues within an organisation. By assessing an organisation's culture, internal auditors can help to create a more ethical, transparent, and inclusive environment for all stakeholders.

10. **Audit of automated processes:** With the increasing use of automation in business processes, internal auditors are being asked to assess the effectiveness of controls put in place to manage the risks associated with automated processes. This includes assessing the effectiveness of automated controls and ensuring that they are properly designed and implemented.

CASE STUDY

Increased Automation in Internal Audit - The Role of Robotics Process Automation (RPA) in Hindustan Unilever Limited (HUL)

Hindustan Unilever Limited (HUL) is a subsidiary of Unilever, a multinational consumer goods company. HUL operates in India and is one of the largest fast-moving consumer goods companies in the country. The company has a robust internal audit process to ensure compliance with regulations, identify potential risks, and make recommendations for improvement. To enhance the effectiveness and efficiency of the internal audit process, HUL implemented Robotics Process Automation (RPA).

The internal audit team at HUL faced several challenges that made it difficult to achieve its objectives. First, the team was heavily reliant on manual processes, which made it difficult to analyse large volumes of data effectively. Second, the team was struggling to keep up with the ever-increasing regulatory requirements, which put a strain on their resources. Third, the team was struggling to identify and mitigate risks in a timely manner, which exposed the company to potential financial and reputational harm.

To address these challenges, HUL decided to implement RPA in the internal audit process. RPA is a software technology that automates repetitive and rule-based tasks that are typically performed by humans. The implementation of RPA has significantly enhanced the effectiveness and efficiency of the internal audit process at HUL.

The RPA system at HUL automates various aspects of the internal audit process, including risk assessment, testing, and reporting. The system uses data analytics and machine learning to identify potential risks and anomalies in large volumes of data, enabling the internal audit team to focus their efforts on the most critical areas of the business. The system also automates the testing process, making it easier for the internal audit team to conduct tests across multiple systems and processes. The automated testing process allows for more comprehensive testing, increasing the accuracy and reliability of the audit results. Finally, the system provides automated reporting, making it easier for the internal audit team to communicate the results of the audit to key stakeholders.

The implementation of RPA in the internal audit process has yielded several benefits for HUL. First, the system has enabled the internal audit team to identify potential risks and anomalies in a more timely and accurate manner, reducing the risk of financial and reputational harm to the company. Second, the automated system has increased the efficiency of the internal audit process, allowing the team to focus their efforts on more critical areas of the business. Finally, the automated reporting process has improved communication with stakeholders, making it easier to ensure that the recommendations of the internal audit team are implemented.

The implementation of RPA in the internal audit process has significantly enhanced the effectiveness and efficiency of the internal audit process at HUL. The use of RPA has enabled the internal audit team to identify potential risks and anomalies in a more timely and accurate manner, reducing the risk of financial and reputational harm to the company. The automated system has increased the efficiency of the internal audit process, allowing the team to focus their efforts on more critical areas of the business. The automated reporting process has improved communication with stakeholders, making it easier to ensure that the recommendations of the internal audit team are implemented. As organisations in India and around the world continue to face ever-increasing complexity and regulatory requirements, it is becoming increasingly important for internal audit teams to embrace automation and leverage the power of data analytics and machine learning to enhance their effectiveness and efficiency.

11. Legal & Company Secretarial

In recent years, legal and company secretarial functions have become increasingly important for internal auditors. This is due to several factors, including the growing complexity of business operations, the

proliferation of regulations and compliance requirements, and the need to ensure that companies are operating ethically and in accordance with their stated values.

Internal auditors are responsible for evaluating a company's internal controls and processes to ensure that they are operating effectively and efficiently. This includes assessing the company's compliance with legal and regulatory requirements, as well as its adherence to ethical standards.

The legal function is concerned with ensuring that a company is complying with all applicable laws and regulations. This includes everything from employment and labor laws to environmental regulations to data privacy and cybersecurity laws. Internal auditors need to be familiar with these regulations and assess whether the company is complying with them.

The company secretarial function is responsible for ensuring that a company is in compliance with its own internal policies and procedures. This includes maintaining accurate records of meetings, ensuring that all relevant documentation is properly filed and stored, and advising on issues related to corporate governance.

Internal auditors need to work closely with legal and company secretarial teams to assess the effectiveness of a company's internal controls and processes. This includes evaluating the company's risk management framework, assessing its internal controls over financial reporting, and evaluating the effectiveness of its compliance program.

In addition to working with legal and company secretarial teams, internal auditors also need to be familiar with emerging areas such as data privacy and cybersecurity. With the proliferation of data breaches and cyber attacks, companies need to ensure that they are protecting their customers' sensitive information and intellectual property.

Overall, the emergence of legal and company secretarial as key focus areas for internal auditors reflects the growing importance of risk management and compliance in today's business environment. By working closely with these teams, internal auditors can help companies stay on top of emerging risks and ensure that they are operating in a responsible and ethical manner.

12. Financial Crime

Financial crime is an emerging area that is increasingly getting into focus in internal audit. Financial crime refers to a broad range of illegal activities that are committed for financial gain, including fraud, money laundering, bribery, corruption, and terrorism financing. The impact of financial crime is significant, as it undermines the integrity of financial systems, damages the reputation of organizations, and poses a threat to national security.

Internal audit plays a crucial role in helping organizations prevent, detect, and investigate financial crime. Internal auditors can assist in identifying and assessing the risks associated with financial crime, evaluating the adequacy of controls, and providing recommendations for improving the effectiveness of the organization's anti-fraud and anti-money laundering measures.

In recent years, there has been an increased focus on financial crime within the regulatory environment, with regulators and governments taking a more proactive approach to combatting financial crime. This has resulted in a growing number of new regulations and guidelines that organizations must comply with, such as the Fifth Anti-Money Laundering Directive in Europe and the Bank Secrecy Act in the United States.

Internal auditors are expected to have a strong understanding of these regulations and guidelines, as well as the emerging trends and risks related to financial crime. This requires ongoing training and development to ensure that internal auditors have the necessary knowledge and skills to effectively identify and address financial crime risks within their organizations.

Financial crime is an emerging area that is getting into focus in internal audit. Internal auditors have an important role to play in helping organizations prevent, detect, and investigate financial crime. By staying up to date with the latest regulations, guidelines, and emerging trends, internal auditors can help their organizations protect themselves against financial crime risks and ensure their ongoing success.

Example 1:

One very prominent example of financial crime that has received significant attention in India in recent years is the Nirav Modi-PNB fraud case. In 2018, it was revealed that the well-known diamond merchant Nirav Modi had fraudulently obtained over $1.8 billion in loans from Punjab National Bank (PNB), one of the largest public sector banks in India.

Nirav Modi and his associates had allegedly obtained these loans by using fraudulent letters of undertaking (LoUs) issued by PNB employees. The LoUs were issued without proper documentation and without following the bank's internal controls and procedures. Modi and his associates then used these funds to finance their business and personal expenses, including the purchase of properties and luxury goods.

The fraud was eventually detected by PNB's internal audit team, which alerted the authorities. The case was then investigated by the Central Bureau of Investigation (CBI) and the Enforcement Directorate (ED), who uncovered a complex web of shell companies, bogus invoices, and other fraudulent transactions.

The Nirav Modi-PNB fraud case highlights the importance of strong internal controls and effective internal audit in preventing and detecting financial crime. It also underscores the need for ongoing training and development for internal auditors to keep up with emerging risks and trends related to financial crime. The case has led to increased scrutiny of banks and financial institutions in India, and has resulted in new regulations and guidelines aimed at improving the effectiveness of anti-fraud and anti-money laundering measures.

Example 2:

Another very famous case of financial crime in India is the Satyam Computer Services fraud case, also known as India's Enron scandal. In 2009, the founder and chairman of Satyam Computer Services, Ramalinga Raju, admitted to having committed financial fraud worth over $1 billion.

Raju had manipulated the company's financial statements by inflating revenues and profits, creating fake invoices, and forging bank statements. He had also misappropriated company funds for personal gain, including the purchase of properties and other assets.

The fraud was eventually uncovered by the company's internal auditors, who alerted the authorities. The case was investigated by the Central Bureau of Investigation (CBI) and the Serious Fraud Investigation Office (SFIO), leading to Raju's arrest and conviction.

The Satyam Computer Services fraud case had significant implications for the Indian corporate sector, as it led to a loss of investor confidence and raised concerns about the quality of corporate governance and internal controls in Indian companies. The case also highlighted the crucial role that internal audit plays in preventing and detecting financial fraud, and the need for ongoing training and development for internal auditors to keep up with emerging risks and trends.

The Satyam Computer Services fraud case resulted in the implementation of new regulations and guidelines aimed at improving the effectiveness of corporate governance and internal controls in India. The case also led to increased awareness of the importance of ethical business practices and transparency in financial reporting.

13. Third Party Risk Management

Third-party risk management is an emerging area of focus in internal audit, and it is gaining more attention due to the increasing reliance on third-party vendors by organizations. Many companies now outsource critical business functions to third-party vendors to reduce costs, increase efficiency, and gain access to specialized expertise. However, this outsourcing exposes organizations to new and evolving risks, such as data breaches, cyber attacks, financial fraud, regulatory non-compliance, and reputational damage.

Internal auditors are responsible for assessing and managing risks within their organizations, and third-party risk management is an area where they can add significant value. Internal audit can help to identify potential risks associated with third-party relationships, evaluate the effectiveness of controls, and make recommendations to management on how to mitigate risks.

In the context of third-party risk management, internal auditors can perform the following key activities:

(i) Assess the adequacy of the organization's third-party risk management program.

(ii) Evaluate the due diligence process for selecting and onboarding third-party vendors.

(iii) Review the contracts and service level agreements with third-party vendors to ensure compliance with regulatory requirements and internal policies.

(iv) Evaluate the effectiveness of monitoring and oversight activities, such as ongoing vendor assessments, audits and reporting.

(v) Analyze the organization's response plan to incidents involving third-party vendors, such as data breaches or disruptions in service.

By focusing on third-party risk management, internal auditors can help organisations ensure that they have the necessary controls in place to manage their relationships with third-party vendors effectively and protect their reputation and assets.

Example:

In early 2021, MobiKwik, one of India's leading mobile wallet and digital payment platforms, suffered a data breach that exposed the personal information of millions of its users. The breach was discovered by a security researcher, who found that MobiKwik's database was being sold on the dark web. The database contained personal information such as names, phone numbers, email addresses, dates of birth, and hashed passwords of millions of MobiKwik users.

The investigation into the data breach revealed that a third-party vendor of MobiKwik, a company called "GigIndia," was responsible for the breach. GigIndia was responsible for providing MobiKwik with a customer verification service, which involved collecting user data and verifying it against government-issued IDs. GigIndia had stored the user data in an unsecured Amazon Web Services (AWS) S3 bucket, which was easily accessible to anyone with the correct URL.

MobiKwik was found to have failed to properly vet and monitor the security practices of GigIndia, and had not ensured that the third-party vendor was in compliance with data protection laws and regulations. The company had also failed to take appropriate action after being notified of the vulnerability by the security researcher.

The data breach had a significant impact on MobiKwik's customers, leading to a loss of trust in the platform, and exposing them to potential fraud and identity theft. The incident also raised concerns among regulatory authorities, who launched an investigation into MobiKwik's data protection practices.

The case study highlights the importance of effective third-party risk management for companies, especially those that handle sensitive user data. Companies that engage with third-party vendors need to implement a robust risk management process that includes:

- **Adequate Due Diligence:** Companies need to conduct thorough due diligence on third-party vendors before engaging with them. This includes verifying their security controls and practices, and ensuring that they are in compliance with data protection laws and regulations.
- **Clear Contractual Provisions:** Contracts between companies and third-party vendors need to include clear provisions that outline specific security requirements and obligations, including data protection, breach notification, and liability.
- **Ongoing Monitoring:** Companies need to establish a process for monitoring third-party vendors regularly to ensure they comply with the contractual provisions, and to detect any potential vulnerabilities or breaches.
- **Effective Incident Response:** Companies need to have an effective incident response plan in place to respond to security breaches effectively, including notifying affected customers, regulators, and law enforcement, and taking appropriate action to mitigate the impact of the breach.

This case focuses and bring out the importance of implementing effective third-party risk management processes to minimise the risks associated with engaging with third-party vendors. Companies need to conduct thorough due diligence on vendors, ensure that contractual provisions are in place to manage risks, regularly monitor vendors, and have an effective incident response plan in place. By doing so, companies can protect themselves from the reputational and financial damage that can result from a breach of third-party vendors.

LESSON ROUND-UP

- Financial accounting is the process of recording, classifying, and summarising financial transactions to provide useful information in making business decisions. The three primary financial statements are the balance sheet, income statement, and cash flow statement. Financial accounting also includes preparing reports for taxation, regulatory compliance, and management decision-making.
- There are several risks associated with financial accounting, which can be broadly categorised into two main types:
    1. Financial risks; and
    2. Funding risks.
- **Financial risks** include the risk of errors or omissions in financial statements, the risk of fraud or misappropriation of assets, and the risk of non-compliance with laws and regulations.
- **Funding risks** include the risk that sufficient funds will not be available to meet obligations when they fall due, the risk of losing access to funding sources, and the risk of incurring additional costs in order to raise additional funds.
- Conducting an internal audit of business can be a challenging task, and some of the common **business-related challenges** that may arise during the process include:
    1. Conflict of Interest

2. Lack of Resources
3. Resistance to Change
4. Limited access to information
5. Complexity of operations
6. Inadequate communication

- Internal audit assignments can be conducted either **in-house or outsourced** to external service providers. Both options have their own advantages and disadvantages, and the decision of whether to use in-house or outsourcing can vary depending on various factors, such as the size and complexity of the organisation, the availability of internal resources, and the cost and quality of external service providers.
- **Co-sourcing** of audit assignments is an approach where an organisation combines in-house resources with external service providers to conduct internal audits. Co-sourcing can provide organisations with the benefits of both in-house and outsourcing options and can be a more flexible and cost-effective approach to internal auditing.
- Emerging Issues
    1. Changing Trends with Time
    2. Disruptive Business Environment
    3. Use of latest Technologies
    4. Right Talent and Skills
- Internal audit is a constantly evolving field, with new areas of focus emerging as organisations and industries change. Some emerging areas getting into focus in internal audit include:
    1. Cyber Security
    2. ESG (Environmental, Social, and Governance)
    3. Artificial Intellegence (AI)
    4. Regulatory and Risk compliance
    5. Supply Chain Risks
    6. Data Privacy
    7. Fraud Prevention
    8. Social Media
    9. Culture Audit
    10. Audit of Automated Process
    11. Legal & Company Secretarial
    12. Finaicial Crime
    13. Third Party Risk Management

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. What is Financial Accounting? Explain the risks involved in Financial Accounting?
2. What is Funding Risks? How it can be avoided?
3. What measures to be taken to avoid financial accounting risk?
4. What are the various business related challenges one can face while conding internal audit?
5. What are the Prons and Cons of In-house Internal Audit function?
6. What are the Prons and Cons of Outsourcing of Internal Audit function?
7. What are the Prons and Cons of Co-sourcing of audit assignment?
8. Why outsourcing is considered as a big risk?
9. Elaborate the various emerging areas to be focused while conducting Internal Audit.

LIST OF FURTHER READINGS

- **Handbook on Internal Auditing**

  Author : CA Kamal Garg

  Publishers : Bharat's
- **Compendium of Standards on Internal Audit**

  Author: ICAI

  Year of Publication: 2022

PART II

FORENSIC AUDIT

Basic Concepts of Forensic Audit

Lesson 10

KEY CONCEPTS

■ Audit ■ Forensic Audit ■ Fraud ■ Fraud Triangle

Learning Objectives

To understand:

- Meaning and Significance of Forensic Audit & the areas cover under Forensic Audit
- What is Audit and its process?
- What are the key advantages of Forensic Audit?
- The need and objectives of Forensic Audit
- The common areas where Forensic Audit can be used
- What are the fundamentals of Forensic Audit?
- The stages of Forensic Audit
- What is Fraud?
- What are the elements of Fraud and Fraud related concept?
- Kinds of Frauds
- Forensic Audit *vis-a-vis* Audit
- Modern Day Scenario

Lesson Outline

- Introduction
- Forensic Audit: Meaning and Significance
- Need and Objectives of Forensic Audit
- Fundamentals of Forensic Audit
- What is Fraud
- Kinds of Frauds
- Forensic Audit vis-a-vis Audit
- Modern Day Scenario
- Case Study
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION

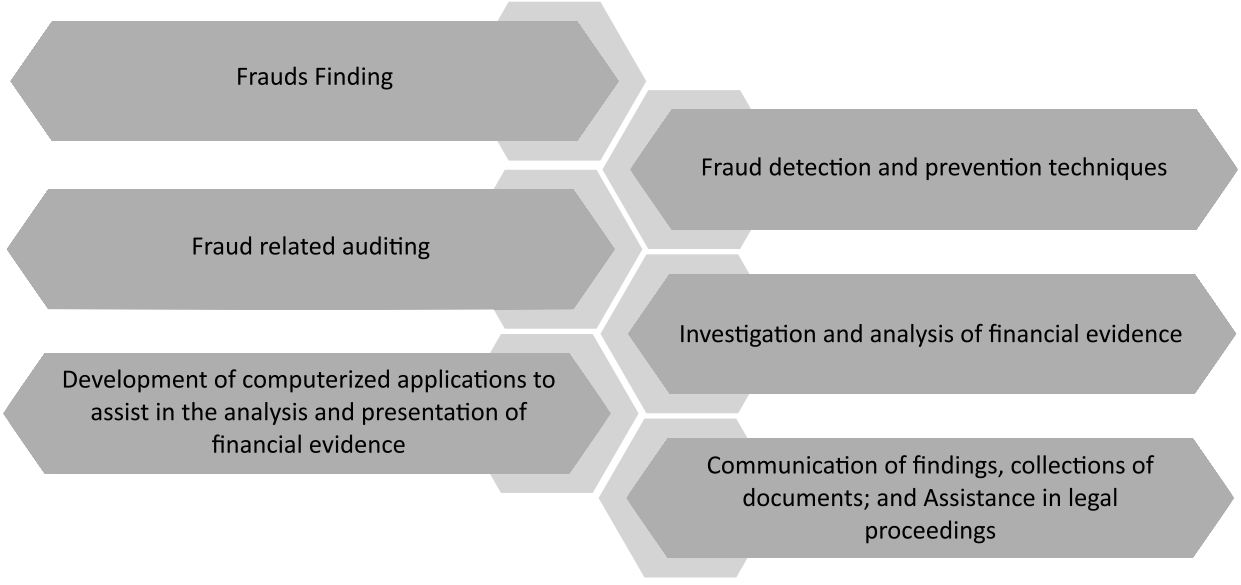
When it comes to auditing, many of organizations consider it is as simply a statutory requirement for getting the financials examined by a certified accountant to ensure compliance. However, this type of audit (financial audit) is just one of many other types of audits that any organization would undergo. Forensic audit is one among such audits which involves an examination of past financial records of an entity to detect any illegal action, manipulation in the books of accounts, siphoning of funds, etc. The forensic audit begins with the suspicion and doubts and ends with the performance of investigation procedures either to confirm the case or dispel the suspicion.

Unlike financial audits which are focused more on statutory compliance, the forensic audits are designed to investigate the financial records of an entity to derive evidences in support of fraud that can be used in court of law or legal proceedings.

In general, Forensic Audit represents an area of finance that combines detective skills and financial acuity. The forensic audit professionals dig deep into financial reports, locate financial transactions and figure out what really happened at various companies and who is the real culprit behind any fraud which has taken place in the company.

Forensic Auditing – It is an independent, comprehensive and scientific approach of reviewing an entity's financial statements in order to determine its accuracy, free from material misstatements and importantly, to derive evidences that can be used in a court of law or legal proceedings.

Forensic Audit cover areas such as:



Further, Forensic Auditing is used in a number of ways and for a number of purposes and not just for criminal activity detection. Firms that do "turn-arounds" or takeovers of businesses, for example, need to have an in-depth understanding of their target's finances. In that scenario, Forensic Audit provides a clear understanding of the financial position along with the connection of the communications related to that.

FORENSIC AUDIT: MEANING AND SIGNIFICANCE

In order to catch the glimpse of Forensic Audit in totality, it also become significant to know and understand the meaning of Audit itself.

Meaning of Audit

Audit, in general, refers to the examination or inspection of various books of accounts by an auditor followed by physical checking of inventory to make sure that all departments are following documented system of recording transactions. It is done to ascertain the accuracy of financial statements provided by the organization.

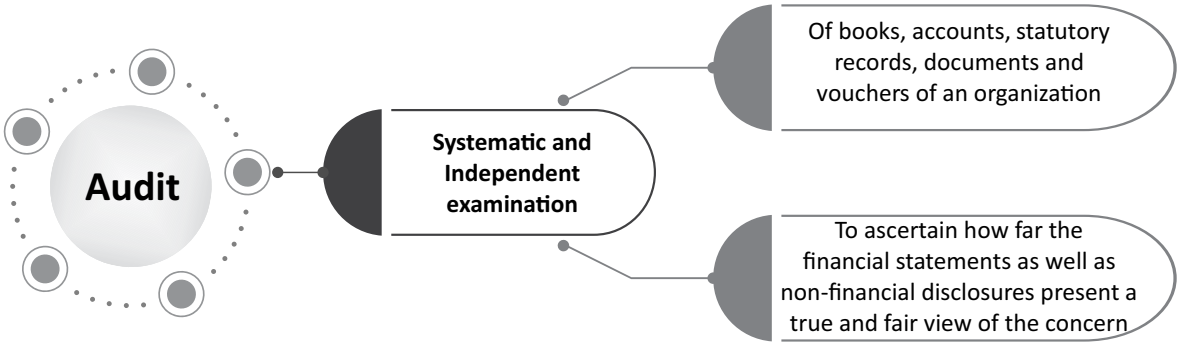
Audit can be done internally by employees or heads of a particular department and externally by an outside firm or an independent auditor. The idea is to check and verify the accounts by an independent authority to ensure that all books of accounts are made in a fair manner and there is no misrepresentation or fraud that is being conducted.

All the public listed firms have to get their accounts audited by an independent auditor before they declare their results for any quarter.

As per *English Oxford Dictionary*, "Audit" means an official inspection of an organization's accounts, typically by an independent body. It also states a word of caution that many a times, audits are not expected to detect every fraud.

Cambridge Dictionary refers that Audit is a systematic process to make an official examination of the accounts of a business and produce a report.

English Oxford Dictionary	Cambridge Dictionary
Audit means - • An official inspection of an organization's accounts, • Typically, by an independent body. It also states a word of cautions that many a times, audits are not expected to detect every fraud.	Audit refers as • Systematic process, • To make an official examination of the accounts of a business, and • To produce a report.



With an analysis of these definitions, it is apt to state that an audit is a systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern.

It also attempts to ensure that the books of accounts are properly maintained by the concern, as required by law.

When we talks about Audit, one should not forget the role of Indian Accounting Standard (abbreviated as Ind-AS). Ind_AS is the Accounting standard adopted by companies in India and issued under the supervision of Accounting Standards Board (ASB) which consists of representatives from government department, academicians, other professional bodies, representatives from ASSOCHAM, CII, FICCI, etc.

The Ind AS are named and numbered in the same way as the International Financial Reporting Standards (IFRS). National Advisory Committee on Accounting Standards (NACAS) recommend these standards to the Ministry of Corporate Affairs (MCA). MCA has to spell out the accounting standards applicable for companies in India. As on date MCA has notified 41 Ind AS. This shall be applied to the companies of financial year 2015-16 voluntarily and from 2016-17 on a mandatory basis.

Based on the international consensus, the regulators will separately notify the date of implementation of Ind-AS for the banks, insurance companies etc.

Audit: An Adhering Significance

The word audit is derived from a Latin word "audire" which means "to hear". During the medieval times when manual book-keeping was prevalent, auditors in Britain used to hear the accounts read out for them and checked that the organization's personnel were not negligent or fraudulent.

Any subject matter may be audited. Auditing is a safeguard measure not only in medieval times, rather it is in existence since ancient times.

Audit provides third party assurance to various stakeholders that the subject matter is free from material misstatement. The term is most frequently applied to audits of the financial information relating to a legal person. Other areas which are commonly audited include, secretarial & compliance audit, internal controls, quality management, project management, water management, and energy conservation.

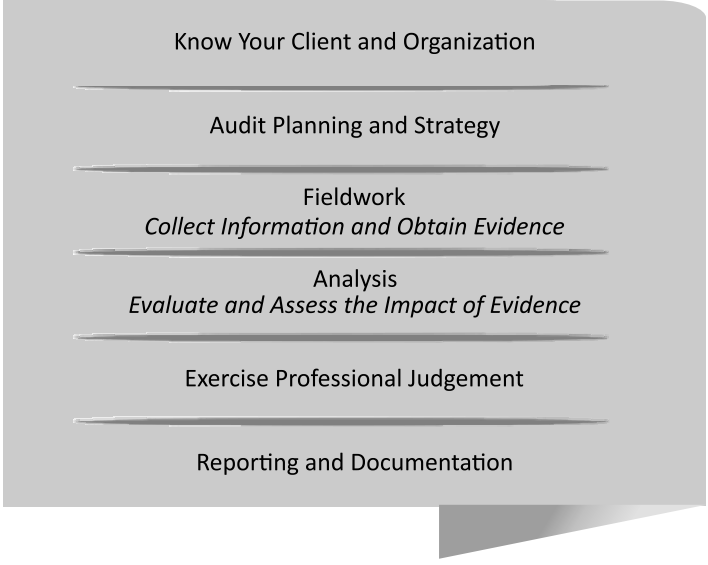
In view of Audits' imperative value for detecting the fraud and ensuing financial health of the corporate, auditing has become such a ubiquitous phenomenon in the corporate and the public sector that professionals started to specialize the process of auditing, wherein forensic audit is also one specialized branch of audit having specific objectives in operation.

During the Audit, the auditor perceives and recognizes the propositions before them for examination, obtains evidence, evaluates the same and formulates an opinion on the basis of his judgment which is communicated through their audit report.

As a result of an audit, stakeholders may effectively evaluate and improve the effectiveness of risk management, control, and the governance process over the subject matter.

Stages of Audit

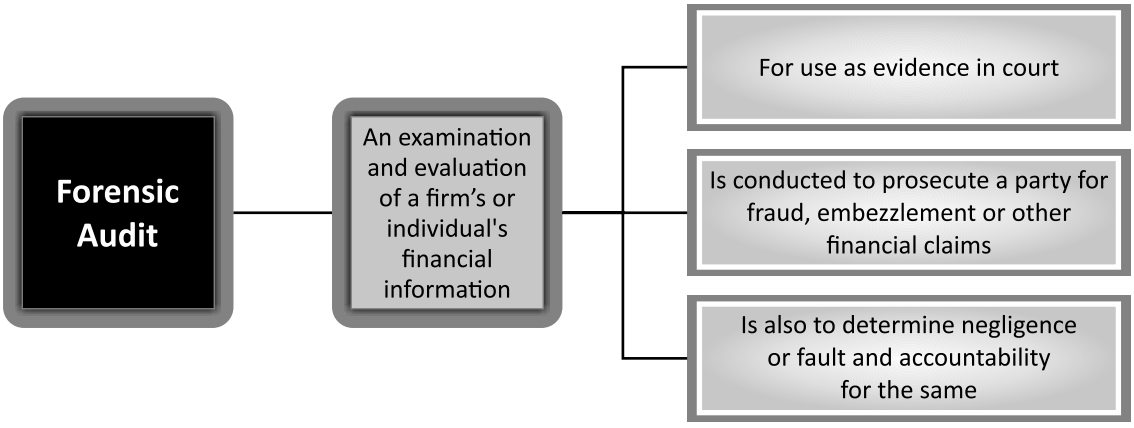
Some Typical Stages in the Audit Process are as below:



Meaning of Forensic Audit

Forensic audit is, in general, referred to as an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court.

As per the definition given in Investopedia, Forensic Audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in court. A Forensic Audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims. In addition, an audit may be conducted to determine negligence or even to determine how much spousal or child support an individual will have to pay.



Jack Bologna and Robert defined Forensic Audit as the application of financial skills and an investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial expertise, fraud knowledge, and a strong knowledge and understanding of business reality and the working of the legal system.

Collin Greenland defines that forensic accounting (or auditing) is the integration of accounting, auditing and investigative skills in order to provide an accounting analysis suitable for the resolution of disputes (usually but not exclusively) in the courts.

Business Dictionary defines Forensic Audit as the application of accounting methods to the tracking and collection of forensic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud. It further states that forensic audit is also called forensic accounting.

Significance of Forensic Audit

Forensic auditing has taken an important role in both private and public organizations since the dawn of the 21st century especially in the advance economies. The catastrophe of some formerly prominent public companies such as Enron and WorldCom (MCI Inc.) in the late 1990s, coupled with the terrorist attacks of September 11, 2001 and the recent incidence of frauds taken place in the corporates including the one in the leading public bank of Indian economy, have fueled the prominence of forensic auditing/ accounting, creating a new, important and lucrative specialty. Forensic auditing procedures target mostly financial and operational fraud, discovery of hidden assets, and adherence to federal regulations.

Cressy (2012) in his paper explained that in forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. Evidence may also be gathered to support other issues which would be relevant in the event of a court case.

Further, with the increase in the financial frauds popularly known as white collar crimes, forensic auditing and

accounting have risen to prominence for ensuring the directed growth of the corporates and inclusive growth of economy.

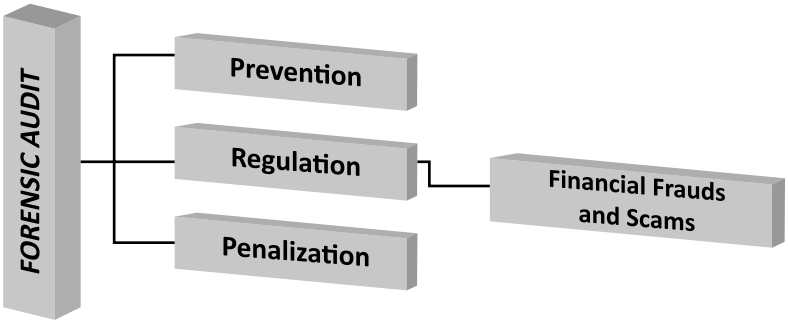
Forensic audit is becoming increasingly frequent for top leadership searches as stringent corporate governance norms and increasing stakes are prompting Indian and multinational companies to make sure that the people they take on board have no blotches on their track record. This realizes the significance of Forensic Audit in the contemporary time for the corporates to rationalize premier principles of Good Governance.

A Ready Reference to the Significance of Forensic Audit could be rationalized as below:

- In general, forensic auditing, which is described as a specialized field of accountancy investigates fraud and analyses financial information to be used in legal proceedings.
- In Forensic Audit, a systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization is held to ascertain fraud or probability of fraud.
- Much beyond the official documents of the company, the Forensic audit involves lot of field work, trying to talk to multiple stake holders to gather information and then look for evidence to corroborate it and alike.
- It also attempts to identify or to corroborate the culprit behind the fraud.
- It arranges and collects the evidences of the fraud and the person accused of fraud.
- The collected evidences and reviewed facts are used in the legal proceedings which assist the court in granting punishment to the real accused of the fraud.
- Forensic auditing uses accounting, auditing, and investigative skills to conduct investigations into theft and fraud. It encompasses both Litigation Support and Investigative Accounting.

This makes forensic audit an apt tool in the contemporary times, ensuring financial health of the companies through aiding in the ***Prevention, Regulation and Penalization*** of financial frauds and scams.

As we have discussed clearly that Forensic Audit is an examination of a company's financial records to derive evidence which can be used in a court of law or legal proceeding. In the contemporary times, when the Government is looking forward for a robust economy and nation building at par, financial stability is a must in the corporates. Henceforth, Forensic audit submits various recompenses in ensuring commercial health of the companies through aiding in the ***Prevention, Regulation and Penalization*** of financial frauds and scams.



For example, A Company, on the recommendation of its Chief Financial Officer (CFO), entered into a contract with ABC Inc for the supply of carts. At the time, ABC Inc was not authorized to conduct business, as its license was suspended due to certain irregularities in taxes paid. The CFO had knowledge of this fact, but still recommended the company to enter into a contract with ABC Inc because he was secretly receiving compensation from ABC Inc for doing so. A forensic audit cannot reveal such cases of fraud, but could also create bunch of evidences

for the production the court of Law. This way forensic audit ensures the healthy conduct of the organization and stability and growth to the economy as a whole.

Key Advantages of Forensic Audit

In this context, few key benefits of Forensic Audit are listed below:

1. **Detection and Responsibility of Corruption:** In a Forensic Audit, while investigating fraud, an auditor would look out for:

   - **Conflicts of interest –** When fraudster uses his/her influence for personal gains detrimental to the company. For example, if a manager allows and approves inaccurate expenses of an employee with whom he has personal relations. Even though the manager is not directly financially benefitted from this approval, he is deemed likely to receive personal benefits after making such inappropriate approvals.
   - **Bribery** – As the name suggests, offering money to get things done or influence a situation in one's favor is bribery. For example, ABC bribing an employee of B2C company to provide certain data to aid ABC in preparing a tender offer to B2C.
   - **Extortion** – If B2C demands money in order to award a contract to ABC, then that would amount to extortion.

   In this process, Forensic Audit aids in detecting the corruption in the corporates and also determine responsibility of the person liable for the corruption and its practices.

2. **Detection of Asset Misappropriation:** This is the most common and prevalent form of fraud. Misappropriation of cash, raising fake invoices, payments made to non-existing suppliers or employees, misuse of assets, or theft of Inventory are a few examples of such asset misappropriation.

3. **Detection of Financial Statement Fraud:** Companies get into this type of fraud to try to show the company's financial performance as better than what it actually is. The goal of presenting fraudulent numbers may be to improve liquidity, ensure top management continue receiving bonuses, or to deal with pressure for market performance. Some examples of the form that financial statement fraud takes are the intentional forgery of accounting records, omitting transactions – either revenue or expenses, non-disclosure of relevant details from the financial statements, or not applying the requisite financial reporting standards.

4. **Fraud Identification and Prevention:** Fraud is quite common in big organizations where the number of daily financial transactions is huge. In such an environment, an employee can easily undertake fraudulent activities without being caught. Forensic accounting helps in analyzing whether the company's accounting policies are followed or not, and whether all the transactions are clearly stated in the books of accounts. Any deviation observed in the books of accounts can help in identifying fraud, and necessary measures can be taken to prevent it in the future.

5. **Making Sound Investment Decisions**: As forensic accounting helps in analyzing the financial standing and weaknesses of a business, it provides a path for investors to make thoughtful investment decisions. A company engaged in fraud is definitely not a good option for investment. Therefore, the reports of forensic accountants act as a guide for potential investors of a company. Many organizations also apply for loans from various financial institutions. By performing an analysis, such institutions can come to a decision on whether they would like to fund a company or not.

6. **Formulation of Economic Policies:** Various cases of fraud that becomes evident after forensic analysis act as a reference for the government to formulate improved economic policies that would be able to curb such fraudulent activities in the future. By doing so, the government can strengthen the economy and prevent such illegal activities in the country.

7. **Rewarding Career Opportunity:** As a career, forensic auditing is extremely rewarding, as it not only involves regular auditing and accounting activities, but also involves identification, analysis, and reporting of the findings during an audit. The acceptance of reports generated by a forensic auditors by the court of law, gives them an upper hand as compared to other accountants. Good forensic auditors are in high demand and can easily draw a striking starting salaries around the globe.

Other Advantages

- **Objectivity and Credibility** – An external party as a forensic auditor would be far more independent and objective than an internal auditor or company accountant who ultimately reports to management on his findings. An established firm of forensic auditors and its team would also have credibility stemming from the firm's reputation, network and track record.
- **Accounting Expertise and Industry Knowledge** – An external forensic auditor would add to the organization's investigation team with breadth and depth of experience and deep industry expertise in handling frauds of the nature encountered by the organization.
- **Provision of Valuable Manpower Resources** – An organization in the midst of reorganization and restructuring following a major fraud would hardly have the full-time resources to handle a broad-based exhaustive investigation. The forensic audit and his team of assistants would provide the much needed experienced resources, thereby freeing the organization's staff for other more immediate management demands. This is all the more critical when the nature of the fraud calls for management to move quickly to contain the problem and when resources cannot be mobilized in time.
- **Enhanced Effectiveness and Efficiency** – This arises from the additional dimension and depth which experienced individuals in fraud investigation bring with them to focus on the issues at hand. Such individuals are specialists in rooting out fraud and would recognize transactions normally passed over by the organization's accountants or auditors.

The above discussed advantages of Forensic Audit confirms that Forensic Audit is a strategical approach in detecting the financial frauds in the organizations along with enhancing their financial stability at par.

NEED AND OBJECTIVES: FORENSIC AUDIT

The punjab national bank has lost the most to frauds in the last five financial years among all the banks in India

Amount lost to frauds (FY13 to FY17)

Punjab National Bank ₹8,999 cr.
State Bank of India ₹6,228 cr.
Bank of Baroda ₹4,412 cr.
Central Bank of India ₹3,944 cr.
Indian Overseas Bank ₹3,339 cr.

Number of frauds (FY13 to FY17)

State Bank of India 2,786
ICICI Bank Ltd. 2,584
HDFC Bank Ltd. 1,146
Bank of Baroda 1,100
Axis Bank Ltd. 1,020

The Kala Ghoda branch of PNB in Mumbai, where the fraud was Reported
■ Emmanual Yogini

Time and again, it has been established that corporate frauds are one of the major hindrances to the inclusive growth of the economy. In any economy the rise in corporate frauds is directly proportionate to the fall of economy. Corporate fraud schemes go beyond the scope of an employee's stated position, and are marked by their complexity and economic impact on the business, other employees and outside parties.

Goldman Sachs on the Impact of PNB Scam on Indian Economy stated that "*To global investors, India's economy may seem a bit like a raw mango these days—enticing from a distance but bitter to taste; good for pickles, and not much more. Indeed, in the days following the revelation that billionaire jewellers, Nirav Modi and Mehul Choksi, duped India's second-largest government bank, the PNB stock has lost more than a quarter of its market value. Other public sector bank scrips have tumbled, too.*"

In the previous years too, India has witnessed financial frauds which affected the golden growth of India's economy. The Investigations and risk consulting firm Kroll unearthed in their survey that 69% of companies studied were affected by fraud in Financial Year of 2013, up from 68% in the previous year. The value of fraud, the study found, rose, to 71% from 67%. Insider fraud was particularly rife in India, with 89% of respondents indicating the perpetrator was an insider of some sort — a junior, middle management or senior employee, or an agent. That's the reason forensic audit practices have evolved significantly over the last 10-15 years. He added that *"earlier the investigations were restricted to books and records but now there is a significant element of intelligence gathering.* The technology, analytics and professional expertise have a greater play in every aspect of forensic auditing".

Indeed, the recent upswing in the financial frauds in India, compelling more management to conduct forensic audits in the interest of our growing economy. Experts on white-collar crimes say forensic auditing is not just gaining prominence, the methods are changing fast.

From all the past incidences, it has been found that Crimes are of all hues, seven in particular — (i) Theft of physical assets, (ii) Theft of information, (iii) Corruption and Bribery, (iv) Internal financial fraud, (v) Vendor fraud, (vi) Management conflict of interest and (v) Regulatory breach, are high in their perspectives of corporate fraud.

As of now, the forensic auditing has emerged as a specialized field in the industry that requires a specific skill set to detect the fraud, leaving no scope for overlap. But, to determine when an organization needs forensic auditing is significant to deal with the early warning signals of fraud. Thus, there are few instances on the occurrence of which an entity should direct for forensic audit like

i. Theft of business information or where business systems have been hacked,

ii. Issues identified by Whistle Blowers,

iii. Reconciliations resulted in unidentified material differences,

iv. Suspicious of fraud or illegal activity,

v. Turnover has occurred and balances are showing negative results.

Forensic Audit is assuming greater importance in India and also globally in the wake of numerous financial frauds, unethical business practices and high incidence of cybercrime. In almost every sector and in verticals, there has been some financial frauds and white-collar crimes, which has paved the way for introducing and adopting the Forensic Audit.

Purpose of Forensic Audit

Lenders / Banks	*Resolution Professional*	*SFIO*	*SEBI*	*CBI*
Misutilization of Funds	Transaction related to Fraudulent trading	Monitory misappropriation	Manipulation of the books of accounts	Misutilization of Funds
Financial Statement Manipulation	Sale/Transfer of assets	Transaction related to Fraudulent trading	False public notices	Financial Statement Manipulation
Sale/Transfer of Assets	Excess payments to related parties	Sale/Transfer of assets & Excess payments to related parties	Insider trading, Price Rigging & Misappropriation of assets	Availing facility through false documentation, False public notices
Availing facility through false documentation via non fund based facilities like LC	Transactions with respect to section 43, 45, 46, 49, 50 and section 66 of IBC	Transactions with respect to section 43, 45, 46, 49, 50 and section 66 of IBC	Cash flow movement, Transaction with group concerns	Excess payments to Management/ Promoters, Siphoning of funds

Common Areas where Forensic Audit is used

With the increase in financial fraud popularly known as white-collar crime, the forensic accounting and auditing has emerged as prominence to ensure the financial growth for businesses and economy as well. Some of the common areas that are to be detected in forensic audit are:-

- **Asset Misappropriation:** Asset misappropriation is the most prevalent form of fraud. Activities such as creating fake invoices to either existing or non-existing suppliers, payments, misappropriation of cash or theft come under the purview of asset misappropriation.
- **Bribery:** Bribery involves offering money to influence a situation or get things done in one's favor.
- **Extortion:** The wrongful use of actual or threatened violence, intimidation or force to gain property or money from an entity or individual. If a fraudster demands the same forcefully then that would amount to extortion.
- **Financial Statement fraud:** Financial statement fraud is the deliberate misrepresentation, misstatement or omission of financial statement data for the purpose of misleading the reader and creating a false impression of an organization's financial strength. The most common practice here is deferring revenues or expense in a different time period to give the appearance of consistent earnings or growth.
- **Conflict of interest:** When a fraudster uses influence for personal gains that prove to be detrimental for the company.

FUNDAMENTALS OF FORENSIC AUDIT

Forensic Auditing in general is referred as a discipline of detecting frauds in the organizations and gathering and presenting financial information in a form of evidences that will be accepted by a court of jurisprudence against perpetrators of economic crimes.

The integration of accounting, auditing, and investigative skills and evidences yields the specialty known as Forensic Auditing which focuses very closely on detecting or preventing financial fraud.

- "Forensic", according to the Webster's Dictionary means, "Belonging to, used in or suitable to courts of judicature or to public discussion and debate."
- The word "Auditing" is defined as the examination or inspection of various books of accounts by an auditor followed by physical checking of inventory to make sure that all departments are following documented system of recording transactions. It is done to ascertain the accuracy of financial statements provided by the organization.

With India being ranked as the 81st in the Global Corruption Perception Index, the needs for forensic audit become all the more profound to strengthen the corporate culture with the vibes of good governance in the country.

The term forensic auditing' refers to financial fraud investigation which includes the analysis of various books of accounts to prove or disprove financial fraud and serving as an expert witness in Court to prove or disprove the same. Thus, basically, the forensic auditing is the use of accounting or secretarial skills for legal purposes.

Major Fundamentals of Forensic Audit involves:

1. An audit
2. An investigation
3. An agreed-upon procedures engagement
4. A proactive search for fraud

1. **Forensic Audit:** - An examination of evidence regarding an assertion to determine its correspondence to establish criteria carried out in a manner suitable to the court. An example would be a Forensic Audit of sales records to determine the quantum of rent owing under a lease agreement, which is the subject of litigation.

2. **Forensic Investigation:** - The utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. A Forensic Investigation may be grounded in accounting, medicine, engineering or some other discipline.

3. **Agreed Upon Procedural Engagement:** As the purpose of the forensic audit is ensure that there is no financial deception in the organizations and it collects evidences after the examination of accounts and its records, therefore, it is required that forensic audit is done under the agreed procedures of Audit and Evidences. For instance for Company Audit, the auditor is required to prepare the audit report in accordance with the Company Auditor's Report Order (CARO) 2016. CARO requires an auditor to report on various aspects of the company, such as fixed assets, inventories, internal audit standards, internal controls, statutory dues, among others.

4. **Predicting the Unpredictable – A Proactive Search:** A Proactive search for fraud comprises a Forensic Audit Thinking. Forensic Audit Thinking involves –

   - The critical assessment throughout the audit of all evidential matter; and
   - Maintaining a higher degree of professional skepticism;
   - That fraud may have occurred, is occurring, or will occur in the future.

   It further involves to decipher pattern, evaluating reports with figures to study their number patterns and comparing them with standards established looking for prima facies area of suspicion.

   In this scenario, Forensic auditing aids in detecting, investigating and preventing the frauds. Whether it is stock market fraud or bank fraud or cyber fraud; forensic auditing seems to be an essential tool for investigation and defining accountability of perpetrators.

Stages of Forensic Audit

Step 1 – Accepting the Investigation

A forensic audit is always assigned to an independent firm/group of investigators in order to conduct an unbiased and truthful audit and investigation. Thus, when such a firm receives an invitation to conduct an audit, their first step is to determine whether or not they have the necessary tools, skills and expertise to go forward with such an investigation. They need to do an assessment of their own training and knowledge of fraud detection and legal framework. Only when they are satisfied with such considerations, can they go ahead and accept the investigation.

Step 2 – Planning the Investigation

Planning the investigation is the key step in a forensic audit. The auditor(s) must carefully ascertain the goal of the audit so being conducted, and to carefully determine the procedure to achieve it, through the use of effective tools and techniques. Before planning the investigation, they should be clear on the final categories of the report, which are as follows:

- Identifying the type of fraud that has been operating, how long it has been operating for, and how the fraud has been concealed
- Identifying the fraudster(s) involved
- Quantifying the financial loss suffered by the client
- Gathering evidence to be used in court proceedings
- Providing advice to prevent the recurrence of the fraud.

Fraud Triangle and Fraud Risk

A fraud triangle is a tool used in forensic auditing that explains three interrelated elements that assist the commission of fraud- Pressure (motive), opportunity (ability to carry out the fraud) and rationalization (justification of dishonest intentions). Fraud risk is the vulnerability a company/organisation has to those who are capable of overcoming the three elements in the fraud triangle. Fraud risk assessment is the identification of fraud risks that exist in the company/organisation. The planning involves the formulation of techniques and procedures that align with the fraud risk and fraud risk management.

Planning also includes the identification of the best way/mode to gather evidence. Thus, it is necessary that ample research is done regarding certain investigative, analytical, and technology-based techniques, and also related legal process, with regard to the outcome of such investigation.

Step 3 – Gathering Evidence

In forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. In order to continue, it is pertinent that the planning stage has been thoroughly understood by the investigating team, who are skilled in collecting the necessary evidence.

The investigators can use the following techniques to gather evidence,

- Testing controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated
- Using analytical procedures to compare trends over time or to provide comparatives between different segments of the business
- Applying computer-assisted audit techniques, for example, to identify the timing and location of relevant details being altered in the computer system
- Discussions and interviews with employees
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

Forensic Data Analysis (FDA)

FDA is the technology used to conduct fraud investigations; the process by which evidence is gathered, summarized and compared with existing different sets of data. The aim here is to detect any anomalies in the data and identify the pattern of such anomalies to indicate fraudulent activity. Such an analysis requires three kinds of expertise,

- Data analyst to perform the technical steps and write the queries
- Team member with extensive experience of the processes and internal controls in the relevant area of the investigated company
- A forensic scientist who is familiar with patterns of fraudulent behaviour.

Step 4 – Reporting

The reporting stage is the most obvious element in a forensic audit. After investigating and gathering evidence, the investigating team is expected to give a report of the findings of the investigation, and also the summary of the evidence and conclusion about the loss suffered due to the fraud. It should also include the plan of the fraud itself, and how it unfolded, basically the whole trail of events, and suggestions to prevent such fraud in the future.

Step 5 – Court Proceedings

The last stage expands over those audits that lead to legal proceedings. Here the auditors will give litigation support as mentioned above. The auditors are called to Court, and also included in the advocacy process. The understanding here is that they are called in because of their skill and expertise in commercial issues and their legal process. It is important that they lay down the facts and findings in an understandable and objective manner for everyone to comprehend so that the desired action can be taken up. They need to simplify the complex accounting processes and issues for others to understand the evidence and its implications.

WHAT IS FRAUD

Fraud is a type of criminal activity, defined as: 'abuse of position, or false representation, or prejudicing someone's rights for personal gain'. Put simply, fraud is an act of deception intended for personal gain or to cause a loss to another party.

The general criminal offence of fraud can include:

- deception whereby someone knowingly makes false representation
- or they fail to disclose information
- or they abuse a position.

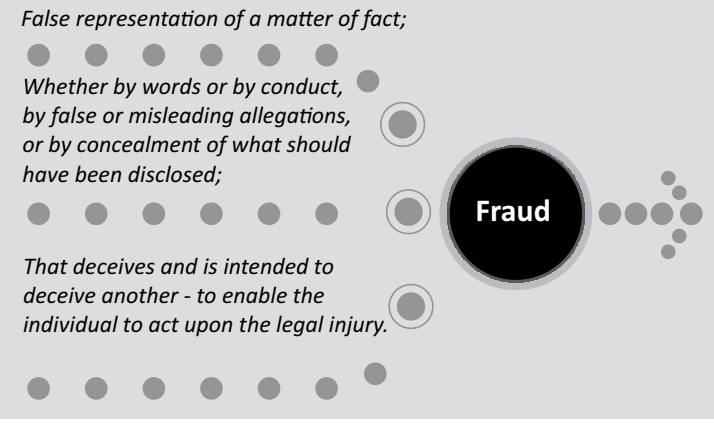
However, incompetence or negligence in managing a business or even a reckless waste of firm's assets (by speculating on the stock-market, for example) does not constitute an act of fraud, but yes, invites legal liabilities. In such cases, if the act of causing financial loss to the business or manipulating the stock market is attempted with the clear intention of deceit, this would tantamount to financial frauds.

In law, fraud is a deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right.

Fraud can also be a civil wrong (*i.e.*, a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal wrong (*i.e.*, a fraud perpetrator may be prosecuted and imprisoned by governmental authorities) or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong.

The ultimate object of practicing fraud may be some monetary gain or other benefit, such as, obtaining a passport or travel document, driver's license or qualifying for a mortgage by way of false statements.

As per Black Law Dictionary, 'Fraud' refers to 'All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling, and any unfair way which another is cheated.



With the clear analysis of the above definitions, it could be asserted that Fraud is a –

- False representation of a matter of fact;
- Whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed;
- That deceives and is intended to deceive another;
- So that the individual will act upon it to her or his legal injury.

'Fraud' is commonly understood as dishonesty calculated for advantage. A person who is dishonest may be called a fraudster. In almost all the legal systems, fraud is a specific offence with certain unique features.

'Fraud' is most commonly practiced in the acts of buying or selling of property, including real estate, personal property, and intangible property, such as, stocks, bonds, and copyrights. Indian law under various statutes criminalizes fraud, but not all cases graduate to the level of criminality. Prosecutors also have discretion in determining which case to pursue and which not. Victims may also seek redress in civil court, provided that the fraud conducted does not affect the society at large. For example, if a fraud is carried out in a company and has adversely affected the profit generation in that company without in any was affecting any counter of the economy, the victims might seek relief under the civil remedy. On the other hand, if the fraud conducted in the company affects the entire economy altogether then the only way to punish the accused is through criminal prosecution against the accused under different criminal law statutes, including the Indian Penal Code, 1860 along with the recovery of amount earned through fraudulent transactions. For instance, in the recent ill-fated Punjab National Bank Scam, CBI added the charges of Criminal Breach of Trust under section 409 of IPC along with charges of Fraud under section 420 IPC, 1860.

As it is clear that fraud is recognized as an act of deceit which is subject to criminal as well as civil legal action in almost all the jurisdictions, including India, hence, it would be apt to discuss the definition and meaning of Fraud under specific laws like Companies Act, 2013, Criminal Procedure Code, 1973 and Indian Penal Code, 1860.

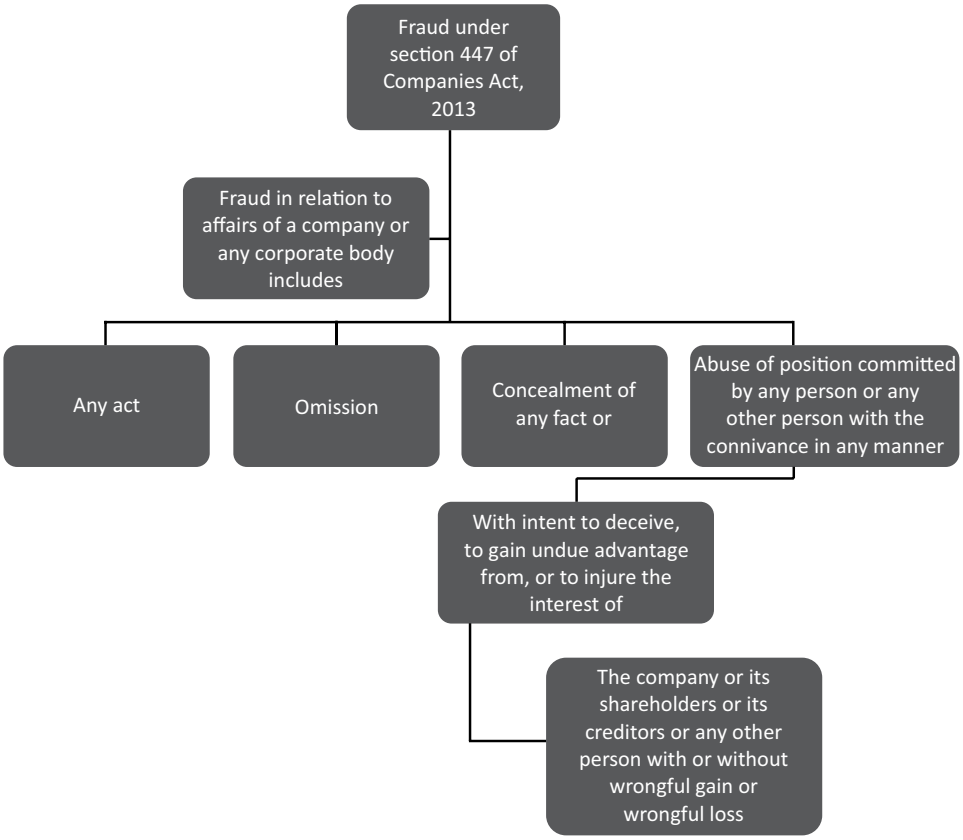
Meaning and Definition under Companies Act, 2013

Explanation of Section 447 of Companies Act 2013 defines Fraud and related terms as below:

(i) 'Fraud' in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

(ii) 'Wrongful gain' means the gain by unlawful means of property to which the person gaining is not legally entitled;

(iii) 'Wrongful loss' means the loss by unlawful means of property to which the person losing is legally entitled.



In the context of this definition, it could be said that Corporate Fraud is a Fraud in relation to affairs of a company or any corporate body as defined in the explanations of Section 447 of Companies Act 2013, which includes

a. Any act,
b. Omission,
c. Concealment of any fact, or
d. Abuse of position committed by any person or any other person with the connivance in any manner, -
    i. with intent to deceive,
    ii. to gain undue advantage from, or
    iii. to injure the interests of,
        a) the company or
        b) its shareholders or
        c) its creditors or any other person

Whether or not there is any wrongful gain or wrongful loss.

Meaning and Definition under Criminal Procedure Code, 1973

The Code of Criminal Procedure, 1973 is the procedural law providing the machinery for punishment of offenders under substantive criminal law. The Code contains elaborate details/provisions regarding the procedure to be followed in every investigation, inquiry and trial, for every offence under the IPC or any other criminal law. In general, the Code does not provide for the definition of various terms rather it only describes certain limited terms like Complaint, Cognizable Offence, Warrant Case and alike, which helps in the interpretation of the Code. For rest of the

terms, section 2(y) of Code says that "words and expressions used herein and not defined but defined in the Indian Penal Code have the meanings respectively assigned to them in that Code." Therefore, to understand the meaning of 'Fraud' in the sphere of criminal law, one has to take recourse of Indian Penal Code, 1860.

Meaning and Definition under Indian Penal Code, 1860

The term 'Fraud' is not defined in the Indian Penal Code per se, but yes Section 25 defines as to what would amount to 'fraudulently'. As per the definition, fraudulently refers – "A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise."

This shows that fraud as a crime is nowhere defined in the Indian Penal Code, but implication of this term is made at various places in Indian Penal Code.

In general, fraud is an act of deliberate deception with the design of securing something by taking unfair advantage of another. It is a deception in order to gain by another's loss.

Whenever the term fraud or defraud appears in the context of criminal law, two things are automatically to be assumed.

- First is deceit or deceiving someone; and
- Second is, injury to someone because of such deceit.

Implications of fraud is found in the following sections of IPC namely, 421, 422, 423 and 424.

- Fraudulent removal or concealment of property to prevent distribution among creditors.
- Fraudulently preventing debt being available for creditors.
- Fraudulent execution of deed of transfer containing false statement of consideration.
- Fraudulent removal or concealment of property.

Though Fraud is not clearly defined in CrPC and IPC, yet Indian Contract Act, 1872 defines the term Fraud quite clearly. In the context of Corporate Fraud, there is no harm in exploring the definition of Fraud as per the other related statutes.

Meaning and Definition under Indian Contact Act, 1872

Section 17 of the Act defines Fraud as –

"Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto his agent, or to induce him to enter into the contract.

Section 17 (1) – the suggestion as to a fact of that which is not by one who does not believe it to be true – is known as *SUGGESTIO FALSI* or suggestion of falsehood.

Section 17 (2) – the active concealment of a fact by one having the knowledge or belief of the fact – is known as *SUPPRESIO VERI* or suppression of a fact.

Section 17 (3) – a promise made without any intention of performing it. It means a promise made falsely with the intention of inducing the other party to make a reciprocal promise and thereby enter into a contract.

Section 17 (4) – any other Act fitted or designed to deceive.

Section 17 (5) – any such act or omission as the law specially declares to be fraudulent

Explanation to Section 17

This explanation states a very important proposition of law. According to Explanation to Section 17 – the mere silence as to a fact likely to affect the willingness of a person to enter into a contract is not fraud. However, such silence is to be held as fraud, if the circumstances of the case that –

- It is the duty of the person keeping silence – to speak
- That his silence in itself is equivalent to speech

Definition of Fraud: The Judicial View

The Supreme Court of India in *Dr. S. Dutt v. State of Uttar Pradesh*, while dilating upon the words "with intent to deceive" has observed that it does not indicate a bare intent to deceive, but an intent to cause a person to act, or omit to act, on account of deception practiced upon him, to his advantage. The words 'but not otherwise' after the words 'with intent to deceive' in the definition of 'fraudulently', it has been observed, clearly show, "..... that the words intent to defraud are not synonymous with intent to deceive and requires some action resulting in some disadvantage which but for the deception, the person deceived would have avoided".

So, under the Indian law a penal offence of fraud, demands for successful prosecution, the twin elements of 'intent to defraud' of the offender *i.e.*—

(i) An intent to deceive another; and

(ii) An intent to cause, by that deception, injury to some person.

Now to clearly understand the term 'fraud' in reference of penalizing, preventing and regulating this act, one should be well-versed with the elements of fraud.

As, it has been thoroughly laid down in the previous discussion that fraud is a termite to growth, development and prosperity, in general, and to the progression of the corporates and economy, in specific. And therefore, the Government is quite dynamic in regulating and preventing the practices of fraud as well as any likelihood of fraud from Indian economy.

In addition, with various laws constituting civil as well as criminal liability for the accused, it is important that fraud should be detected at the first instance and further accused should be penalized with the appropriate punishment in order to introduce the element of deterrence for the anticipated fraudsters, while preventing them from playing any fraud in future.

This all requires a diligent set of skills and tools for detecting the fraud through transactions outside the system reflecting fraud, through analysing the financial statements and other circumstantial evidences making the difference in identifying fraudulent disclosure and finding the real culprit behind the fraud and related loss, providing the evidences in the court and in toto helping the governance of the company with regulation and prevention of frauds in the company. *This consolidated tool is known as Forensic Audit.*

Elements of Fraud

Few Essential Elements of Fraud are listed as below:

1. **False and Wilful representation or Assertion**: To constitute fraud there must be some representation or assertion, which is untrue. In the absence of representation or assertion except in the following two cases, there can be no fraud.

   - Where silence may itself amount to fraud, and
   - Where there is active concealment of facts.

   The person making the representation should not believe it to be true, otherwise he/she will not be guilty of fraud. Moreover, to constitute fraud, the false representation must have been made wilfully or intentionally. For example, X, intending to deceive Y, informs him that his estate is free from encumbrance. Y thereupon buys the estate. The estate is, however, subject to mortgage. The contract is induced by fraud.

2. **Perpetrator of Representation:** The false representation or misstatement must have been made by a party to the contract or by anyone with its connivance, or by its agent. If a stranger makes the misstatement to the contract, it cannot result in fraud. For instance, A suggests B to buy C's car, which according to A runs 15 kms per litre. Later on, B finds that the car runs only 8 kms per litre. A was, however, acting neither at the instance of C nor was his agent; he was a stranger. The contract that took place between B and C cannot be stated to be induced by fraud.

3. **Intention to deceive:** Intention to deceive the other party is the essence of fraud. In order to commit a fraud, one person asserts or misstates the fact with the intention that it should be acted upon. As a matter of fact, misrepresentation elevates to the level of fraud when it is prefixed by the element of intention to deceive the other party. For example, A, intending to deceive B, falsely represents that 1,000 tons of sugar is produced annually at his factory, although A is fully aware that only 600 tons of sugar can be produced annually. B thereby agrees to buy the factory. A has resorted to fraud to obtain the consent of B.

4. **Representation must relate to a fact:** The representation made by the party must relate to a fact, which is material to the formation of the contract. A mere statement of opinion, belief, or commendation cannot be treated as fraud. For instance, A states that the detergent produced at his factory washes whiter than whitest. The statement made by A is merely a commendation of the product and not a fact. But if A describes the ingredients, which the detergent contains, it becomes a statement of fact. And if that is found incorrect, it amounts to fraud provided A knows it to be a false statement.

5. **Active concealment of facts:** 'Active concealment' must be distinguished from 'passive concealment'. Passive concealment implies mere silence as to material facts, which barring a few cases, does not amount to fraud. Whereas, active concealment implies 'when the party takes positive or deliberate steps to prevent information from reaching the other party and this is treated as fraud.' For example, A sells a horse to B in an auction despite knowing that the horse is unsound. A says nothing to B about the horse's soundness. This is a case of passive concealment of fact and cannot tantamount to fraud.

6. **Promise made without intention of performing it:** If a person while entering into a contract has no intention to perform his/her promise, there is a fraud on his/her part, for the intention to deceive the other party is there from the very beginning. For example, an English merchant appointed an Indian woman as his

personal secretary and promised that he would marry her. Later she came to know that he was already married and had made the promise without any intention to perform it. It was held that she could avoid the contract on the ground of fraud.

On similar count, a purchase of goods without any intention of paying the price is a fraud and the contract can be avoided on this ground.

7. **Representation must have actually deceived the other party:** The representation made with the intention to deceive must actually deceive. The party, induced by fraudulent statement, must have relied on it to accord its consent.

   Thus, an attempt to deceive does not amount to fraud until the other party is deceived thereby. A case in point is the following example. A had a defective cannon. With a view to conceal the defect, he put a metal plug on it. B without examining it bought it. The cannon burst when used by B. B refused to pay the price and accused A of fraud. It was held that B was bound to pay because he was not actually deceived, as he would have bought the cannon even if the deceptive plug had not been inserted.

8. **Any other act fitted to deceive:** The expression 'any other act fitted to deceive' obviously means any act, which is done with the intention of committing fraud. This category includes all tricks, dissembling, and other unfair ways, which are used by cunning and clever people to cheat others. For example, a husband persuaded his illiterate wife to sign certain documents telling her that by the papers he was going to mortgage her two plots of land to secure his indebtedness. But, in fact, he mortgaged four plots of land belonging to her. This was held as an act done with the intention of deceiving the wife.

9. **Any such Act or omission that the law specially declares as void:** This category includes the act or omission that the law specially declares to be fraudulent. For example, the Insolvency Act and the Companies Act declare certain kinds of transfers to be fraudulent. Similarly, under the Transfer of Property Act, the transferor of real estate is bound to disclose to the transferee the following details:

   - Material defects, if any, in the property such as, cracks in the wall or in beams, and/or
   - Any defect or dispute as regards transferor's title, such as property is subject to encumbrance, i.e., mortgaged or is subject to some dispute pending in a court of law. An omission to make such disclosure on the part of transferor amounts to fraud.

10. **Wrongful Loss and Wrongful Gain is Immaterial.** For the purposes of "Fraud" under the Companies Act, 2013, it is immaterial whether there has been some wrongful loss to one and/or wrong gain to another. The only important thing is intention to deceive and the act or omission actually deceiving the victim. Common corporate frauds for example are, if the CMD husband benefits from a loan transaction sanctioned by her it is a fraud. If a CEO take bribe to approve a contract that is a fraud.

    On the same principle, Indian Penal Code too works, as for IPC to constitute an offence, two elements are required which are *Mens Rea* – Intention to Commit Offence and *Actus Reus* – The Wrongful Act.

Examples – Corporate Fraud

There are a number of ways in which a corporation can commit fraud. Corporate fraud can encompass the loss of assets by a corporation, or acts perpetrated by the corporation to take funds from others. Here are several examples:

- **Personal purchases.** An employee can divert funds to buy goods or services on his own behalf. This is usually done by approving his own expense reports or supplier invoices. The person must hold a sufficiently senior position to be able to browbeat other employees into participating in this diversion of assets. Usually, the potential amount of funds diverted increases with the seniority of the job title of the individual committing the fraud.

- **Ghost employees.** The payroll staff can create fake employees and then pay these "ghost employees," directing the funds into their own bank accounts. Weak controls over the payment of employees makes this type of fraud more likely.
- **Skimming.** Incoming funds are intercepted before they can be recorded in a company's accounting records. This is usually caused when a person is allowed to both open the mail and record accounting transactions.
- **Tax avoidance.** A company can alter its tax returns to reveal less taxable corporate income than is really the case, resulting in lower tax remittances. This can only be done with the connivance of senior management, which typically signs off on the tax returns.
- **Asset theft.** Any employee can steal from an organization by making off with assets, such as cash or fixed assets. Weak controls can encourage employees to engage in this activity.
- **Unauthorized use.** An employee may use company assets in an unauthorized manner, such as driving a company car for personal use, or using a company condominium for personal use. Though the asset is not stolen, it is being consumed, so its value lessens over time.
- **Financial statement falsification.** An organization can falsify its financial statements to reveal excellent financial results. These documents can then be used as the basis for obtaining bank loans or selling stock to investors. Such falsification can be conducted entirely within the accounting department, or be forced upon it by management. Examples of such falsification are:
  - Extending the depreciation period to delay depreciation recognition
  - Shifting debt to special purpose entities
  - Accelerate the recognition of revenues and delay the recognition of expenses
  - Capitalize expenses
  - Counting nonexistent inventory, which reduces the cost of goods sold.

Corporate fraud can be extremely difficult to contain, and is essentially impossible to stop if senior management is willing to engage in it. In such cases, even the most robust control systems can be breached. This contemplates the significance of Forensic Audit, wherein a check and vigil mechanism could be establishing in finding out the probability of fraud as well as real culprit behind corporate frauds.

Fraud and Forensic Audit: An Introspect

Forensic auditing covers a broad spectrum of activities, with terminology not strictly defined in regulatory guidance. Generally, the term 'forensic auditing' is used to describe the wide range of investigative work which the professionals in practice could be asked to perform. The work would normally involve an investigation into the financial affairs of an entity and is often associated with investigations into alleged fraudulent activity.

- Forensic Auditing refers to the whole process of investigating a financial matter, including potentially acting as an expert witness if the fraud comes to trial.
- The process of forensic accounting includes the 'forensic investigation' itself, which refers to the practical steps that the forensic auditor takes in order to gather evidence relevant to the alleged fraudulent activity.
- The investigation is likely to be similar in many ways to an audit of financial information, in that it will include a planning stage, a period when evidence is gathered, a review process, and a report to the client.

- The purpose of the investigation, in the case of an alleged fraud, would be to discover-
  a. If a fraud had actually taken place,
  b. To identify those involved,
  c. To quantify the monetary amount of the fraud (i.e. the financial loss suffered by the client), and
  d. To ultimately present findings to the client and potentially to court.
- Finally, 'forensic auditing' refers to the specific procedures carried out in order to produce evidence.
- Audit techniques are used to identify and to gather evidence to prove, ***for example,*** "how long the fraud has been carried out, and how it was conducted and concealed by the perpetrators."
- Evidence may also be gathered to support other issues which would be relevant in the event of a court case. Such issues could include:
  a. The suspect's motive and opportunity to commit fraud
  b. Whether the fraud involved collusion between several suspects
  c. Any physical evidence at the scene of the crime or contained in documents
  d. Comments made by the suspect during interviews and/or at the time of arrest
  e. Attempts to destroy evidence.

Fraud Related Concept

Fraud is an independent civil as well as a criminal offence, but it also appears in different contexts as the means used to gain legal advantage or accomplish a specific crime. For example, it is fraud for a person to make a false statement on a license application in order to engage in the regulated activity. A person who did so would not be convicted of fraud. Rather, fraud would simply describe the method used to break the law or regulation requiring the license.

Fraud must be proved by showing that the defendant's actions involved five separate elements:

(1) A false statement of a material fact,

(2) Knowledge on the part of the defendant that the statement is untrue,

(3) Intent on the part of the defendant to deceive the alleged victim,

(4) Justifiable reliance by the alleged victim on the statement, and

(5) Injury to the alleged victim as a result.

These elements contain nuances that are not all easily proved. And that is the reason the tool of forensic audit is effective in identifying the fraud, proving the fraud, determining accountability of the malefactors of fraud and assisting the court of law in penalizing the wrongdoers.

In order to understand the fraud in clarity, one must go through the frauds related concepts which are described as below:

- **First,** not all false statements are fraudulent. To be fraudulent, a false statement must relate to a material fact. It should also substantially affect a person's decision to enter into a contract or pursue a certain course of action. A false statement of fact that does not bear on the disputed transaction will not be considered fraudulent.

- **Second,** the defendant must know that the statement is untrue. A statement of fact that is simply mistaken is not fraudulent. To be fraudulent, a false statement must be made with intent to deceive the victim. This is perhaps the easiest element to prove, once falsity and materiality are proved, because most material false statements are designed to mislead.
- **Third,** the false statement must be made with the intent to deprive the victim of some legal right.
- **Fourth,** the victim's reliance on the false statement must be reasonable. Reliance on a patently absurd false statement generally will not give rise to fraud; however, people who are especially gullible, superstitious, or ignorant or who are illiterate may recover damages for fraud if the defendant knew and took advantage of their condition.
- **Finally,** the false statement must cause the victim some injury that leaves her or him in a worse position than she or he was in before the fraud. A statement of belief is not a statement of fact and thus is not fraudulent. Puffing, or the expression of a glowing opinion by a seller, is likewise not fraudulent. For example, a car dealer may represent that a particular vehicle is "the finest in the lot." Although the statement may not be true, it is not a statement of fact, and a reasonable buyer would not be justified in relying on it.
- **Further, the relationship between parties can make a difference in determining whether a statement is fraudulent.** A misleading statement is more likely to be fraudulent when one party has superior knowledge in a transaction, and knows that the other is relying on that knowledge, than when the two parties possess equal knowledge.

  For example, if the seller of a car with a bad engine tells the buyer, the car is in excellent running condition, a court is more likely to find fraud if the seller is an auto mechanic as opposed to a sales trainee. Misleading statements are most likely to be fraudulent where one party exploits a position of trust and confidence, or a fiduciary relationship. Fiduciary relationships include those between attorneys and clients, physicians and patients, stockbrokers and clients, and the officers and partners of a corporation and its stockholders.
- **A statement need not be affirmative to be fraudulent.** When a person has a duty to speak, silence may be treated as a false statement. This can arise if a party who has knowledge of a fact fails to disclose it to another party who is justified in assuming its non-existence.

  For example, if a real estate agent fails to disclose that a home is built on a toxic waste dump, the omission may be regarded as a fraudulent statement. Even if the agent does not know of the dump, the omission may be considered fraudulent. This is constructive fraud, and it is usually inferred when a party is a fiduciary and has a duty to know of, and disclose, particular facts.
- Fraud resembles theft in that both involve some form of illegal taking, but the two should not be confused. Fraud requires an additional element of False Pretenses created to induce a victim to turn over property, services, or money. Theft, by contrast, requires only the unauthorized taking of another's property with the intent to permanently deprive the other of the property. Because fraud involves more planning than does theft, it is punished more severely.

The above discussion clarifies, that the menace of fraud is not easy to detect and it may be mean different acts, omissions and offences under different circumstances and further it requires vibrant evidences to prove the conduct as fraud. In these circumstances, forensic audit aids for detection and gathering evidence of frauds, embezzlement, or any other such white-collar crime. It is the application of accounting skills to legal questions. And with this kills of ensuring financial stability in both public and private organizations, especially in advanced economies, forensic audit is the need of the hour.

KINDS OF FRAUDS

Fraud in general could be categorized in two category in legal parlance, which includes

1. Fraud as a Civil Wrong and
2. Fraud as a Criminal Offence.

1. ***Fraud as a Civil Wrong,*** is a tort. While the precise definitions and requirements of proof vary among jurisdictions, the requisite elements of fraud as a tort generally are the intentional misrepresentation or concealment of an important fact upon which the victim is meant to rely, and in fact does rely, to the harm of the victim. Proving fraud in a court of law is often said to be difficult. That difficulty is found, for instance, in that each and every one of the elements of fraud must be proven, that the elements include proving the states of mind of the perpetrator and the victim, and that some jurisdictions require the victim to prove fraud by clear and convincing evidence.

The remedies for fraud may include rescission (i.e., reversal) of a fraudulently obtained agreement or transaction, the recovery of a monetary award to compensate for the harm caused, punitive damages to punish or deter the misconduct, and possibly others.

In cases of a fraudulently induced contract, fraud may serve as a defense in a civil action for breach of contract or specific performance of contract. Fraud may serve as a basis for a court to invoke its equitable jurisdiction.

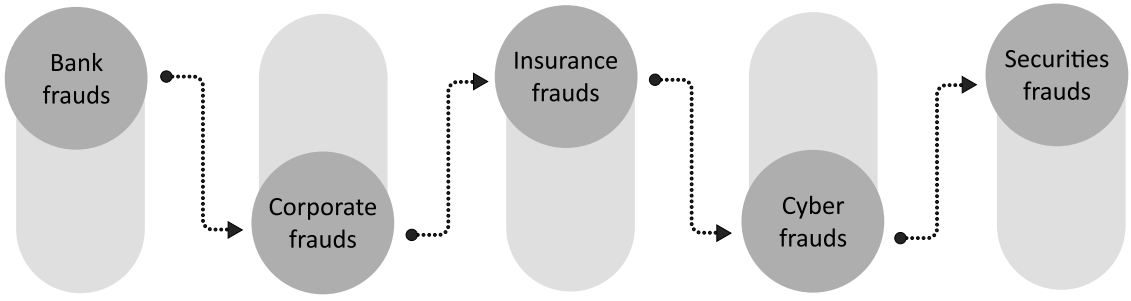
2. ***Fraud as a Criminal offence***, takes many different forms, some general (e.g., theft by false pretense) and some specific to particular categories of victims or misconduct (e.g., bank fraud, insurance fraud, forgery). The elements of fraud as a crime similarly vary. The requisite elements of perhaps the most general form of criminal fraud, theft by false pretense, are the intentional deception of a victim by false representation or pretense with the intent of persuading the victim to part with property and with the victim parting with property in reliance on the representation or pretense and with the perpetrator intending to keep the property from the victim. In Indian Law, Implications of fraud is found in these following sections of IPC namely, 421,422,423 and 424.

- Fraudulent removal or concealment of property to prevent distribution among creditors
- Fraudulently preventing debt being available for creditors.
- Fraudulent execution of deed of transfer containing false statement of consideration.
- Fraudulent removal or concealment of property.

Kinds of Fraud in specific to Economy and Financial Transactions

In specific to the impact on economy and financial transactions, frauds could be categorized as below:

1) Bank frauds
2) Corporate frauds
3) Insurance frauds
4) Cyber frauds
5) Securities frauds



1) **Bank Frauds**: Bank fraud is a big business in today's world. The number of bank frauds in India is substantial. It is in increasing with the passage of time in all the major operational areas in banking. There is different area in Bank Deposits, loan, inter branch, accounting, transaction etc.

2) **Corporate Frauds**: In India, Corporate Frauds from leading Indian business are shaking the economy time and again. From Satyam Computers stunned the national financial world in 2009, when Satyam's Founder B. Ramalingan Raju declared he had inflated profit and jacked up the company's Balance Sheet by more than one billion dollars to the recent incident of PNB Fraud in year 2017, Frauds are apparent in the corporates. This needs to be checked strictly to ensure financial stability and emerging economy.

3) **Insurance Frauds**: There is different type of frauds in insurance sectors. E.g. health insurance, claims fraud, false claims, insurance speculations, application frauds etc.

4) **Cyber Frauds**: Cyber Frauds are the frauds done with the help of the internet targeting the unauthorized use of digital instruments like credit card, ATM card, cyber equipment's at home etc.

5) **Securities Frauds**: Apart from Corporate Frauds, Frauds in the Securities and Securities Market are also affecting many people time and again. From the perspective of frauds in securities, investor community could not forget the under truncate Rs. 4000 crore of Harshad Metha scam and over Rs. 1000 Crore of Ketan Parekh scams which duped the shareholder with the loss of their wealth in the big markets. In addition to this, the instances of Insider trading are also considered securities fraud in many circumstances.

Corporate Frauds: An Insight

Fraud against a company can be committed either internally by employees, managers, officers, or owners of the company, or externally by customers, vendors, and other parties. Other schemes defraud individuals, rather than organizations.

Internal Fraud: Internal fraud, also called occupational fraud, can be defined as: "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets." Simply stated, this type of fraud occurs when an employee, manager, or executive commits fraud against his or her employer.

External Fraud: External fraud against a company covers a broad range of schemes. Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees. Likewise, dishonest customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund. In addition, organizations also face threats of security breaches and thefts of intellectual property perpetrated by unknown third parties.

As reported time and again with various incidents like that of Nirav Modi in the early month of 2018, of Vijay Mallya, of Sahara Subrato Rao, of Satyam Computers, of 2G and alike, Corporate Scams are affecting the economic health of the companies time and again. With nearly over 250 scams in India since 1947, an approximate of 20.23 Trillion US Dollar loss has been reported in Corporate Scams in India.

Deccan Chronicle in its latest article reported that India has seen a significant rise in incidence of fraud, cyber and security related incidents, which according to a private survey is higher than the global average. Around 89 per cent of the respondents in India who participated in the Kroll global fraud survey report said that they had experienced a fraud incident in the past one year. Respondents in India reported one of the world's highest incidences of theft of physical assets or stock, with two-fifths saying they had experienced this type of fraud, second only to those in Canada. Theft of intellectual property and market collusion are also high on the list of incidents of fraud in India. What is more interesting is that a higher proportion of respondents (45 per cent) in India cited joint venture partners as the main reason for increased exposure to fraud while 43 per cent attributed the role of junior employees for the likely occurrence of frauds.

According to the survey, India figures among the top three countries globally for every category measuring fraud vulnerability except for vendor, supplier, or procurement fraud. Nearly nine in 10 respondents (87 per cent) cited information theft, loss, or attack as their greatest concern, 30 percentage points higher than the global average of 57 per cent.

Internal financial fraud, IP theft, piracy, and counterfeiting were also significantly higher than the global averages. However, the survey noted that Indian corporates are becoming more aware of the risks and are implementing preventive measures such as financial controls and physical security systems. Coming to cyber related frauds, 84 per cent of the respondents said they experienced a cyber-attack in the last one year. Nearly half of these respondents experienced email-based phishing attacks. Virus/worm attacks were the second most common type of incident reported. The most common targets for cyber-attacks in India were employee records, trade secrets or intellectual property and customer records. Henceforth, there seems an urgent need to implement the tool of forensic audit, which would be a great check on these frauds and in turn would boost the economy of the nation.

Live Cases

1. FORENSIC AUDIT ON PNB SCAM

Punjab National Bank appointed a BDO to conduct a forensic audit of jeweler Nirav Modi's companies, according to people directly briefed on the matter.

The bank issued a formal appointment letter to the Belgium-headquartered audit firm on February 27, 2018 to conduct a forensic audit in the scam wherein Modi, his uncle Mehul Choksi and their companies have been accused of defrauding the bank of as much as Rs 12,700 crore.

In the starting of January, 2018, PNB informed the BSE (Bombay Stock Exchange) that it has detected some "fraudulent and unauthorized transactions" in one of its branches in Mumbai to the tune of $ 1771.69 million (approx.). Following the announcement, the share price of the state-owned bank plunged 10%.

Meanwhile, the Central Bureau of Investigation (CBI) received two complaints from PNB against billionaire diamantaire Nirav Modi and Jewelry Company alleging fraudulent transactions worth about Rs. 11, 400 crores, the Press Trust of India reported. This is in addition to the Rs. 280 crore fraud case that he is already under investigation for, again filed by PNB.

Nirav Modi, the billionaire in the middle of this controversy, is a luxury diamond jewelry designer who was ranked #85 in the Forbes list of India's billionaire in 2017.

The Modus Operandi

- In a statement issued to stock exchanges, PNB said it has detected some "fraudulent and unauthorized transactions (messages)".
- A stock statement is a business statement that provides information on the value and quantity of stock related transactions. It details opening and closing balances for transacted items as well.

According to the complaint filed by PNB with the CBI on January 28, the fraudulent issuance of Letters of Undertakings (LOU) was detected at the Mid Corporate branch, Brady House in Mumbai.

2. FORENSIC AUDIT ON DENA BANK

The Finance Ministry has ordered a forensic audit of Dena Bank and Oriental Bank of Commerce after some of their Mumbai-based branches allegedly misappropriated funds worth Rs. 437 crore, mobilised through fixed deposits. Professional services firm KPMG in India has been given the mandate to undertake forensic investigations. In the case of Dena Bank, the misappropriation was to the tune of Rs. 257 crore and related to funds mobilised from seven corporate. In Oriental Bank's case, it related to misappropriation of funds amounting to Rs. 180 crore, reportedly belonging to the Jawaharlal Nehru Port Trust. The Central Bureau of Investigation is already looking into the alleged fraud. The developments are disparate ones and took place at different times. But a common feature could be that they centered on mobilising deposits: fixed deposits/bulk deposits. The incidents have again brought to the fore the weak risk management systems in public sector banks. "The persons responsible have been taken to task; some disciplinary action is being taken. There are also some suspensions, some transfers...."

Directors' Responsibilities

The ubiquitous issue of corruption and the high risk of internal fraud raise serious concerns about the liability of corporate directors. India has learned a lot in recent years, and its laws have gradually evolved in this context.

Director liability in India can be divided into two principal areas:

(1) liability under the Companies Act 2013 (the 2013 Act); and

(2) Liability under other Indian statutes.

There has been a seminal shift in the Indian corporate legal regime with the enactment of the 2013 Act and more recent amendments.

For instance:

- Penalties under the erstwhile Companies Act 1956 that were seen as ineffective have been significantly amplified under the Companies Act, 2013.
- The Companies Act, 2013 also provides statutory recognition to the duties of a director, such as exercise of due and reasonable care, skill, diligence, and independent judgment.
- One of the key concepts of the Companies Act is the meaning of the term "officer who is in default." Under the act, liability for default by a company has been imposed on an officer who is in default.
- By virtue of their positions in the company, the managing director, the whole-time director, and the company secretary directly fall within the scope of this term.
- Under the erstwhile Companies Act, 1956 certain key employees such as the chief executive officer and chief financial officer did not directly come within the ambit of the term, which raised serious concerns because these personnel were viewed as key officials in any company.
- The Companies Act, 2013 corrects this anomaly and significantly expands the scope of the expression "officer in default." The term also includes the following:
    i. any individual who, under the superintendence, control, and direction of the board of directors, exercises the management of the whole, or substantially the whole, of the affairs of a company;
    ii. any person on whose advice, directions, or instructions the board of directors is accustomed to act, other than persons giving advice in a professional capacity; and

iii. Every director aware of wrongdoing by virtue of knowledge of or participation in proceedings of the board without objection.

This way, under Companies Act, 2013, the scope of Director Responsibility has been expended to stop the tendencies of fraud in the Corporates. Directors can be held liable both jointly and collectively, for any and every act, commission or omission which is prejudicial to the interests of the company and violates any of the duties to be discharged by them.

A ready reference of Directors Responsibility could be chalked as under:

Director's Personal Liability

As a general rule, since the company and its Director are separate entities, the Director has no personal liability on behalf of the company. However, under certain circumstances, a Director may be held liable on behalf of the company. These circumstances are:

- Liability for Tax
- Debts of the Company
- Liability for company's Contracts
- Refund of Share application Money
- Liability to pay for qualification shares
- Mis-statement in the Prospectus

Fraudulent Conduct of Business: A Director may be held personally responsible, without any limitation of liability, for all or any of the debts or other liabilities of the company if he or she was knowingly party to the fraudulent carrying on of business.

Unlimited Liability: The liability of any or all of the Directors of a limited company can be unlimited if so provided by the Memorandum, or can be so done if approved by a special resolution as authorized by the Articles.

FORENSIC AUDIT VIS-À-VIS AUDIT

Major difference between Audit and Forensic Audit is discussed as below:

- Objective of financial auditing is to express opinion as to 'true & fair' presentation. Forensic Audit determines correctness of the accounts or whether any fraud has actually taken place.
- Techniques used in the financial auditing are more of 'Substantive' and 'compliance' procedures. The techniques used in the forensic auditing are analysis of past trend and substantive or 'in depth' checking of selected transactions.
- Normally all transactions for the particular accounting period are covered under the financial audits. Forensic audits don't face any such limitations. Forensic auditors may be appointed to examine the accounts from the beginning.
- For ascertaining the accuracy of the current assets and the liabilities financial auditor relies on the management certificate or representation of management. Forensic auditors are required to carry out the independent verification of suspected or selected items.
- Whenever the financial auditor has adverse findings, then the auditor expresses the qualified opinion, with/without quantification. In case of the adverse findings, the forensic auditors are required to quantify the damages to the clients and is also supposed to point the culprit. Many a times, Legal action will be sought.

MODERN DAY SCENARIO

It is always said that to ensure the availability of best means of livelihood and to provide citizens with virtues of 'Justice' and 'Welfare', which also results in the inclusive growth of nation as a whole, the prerequisite is that there must be a relationship of trust and faith *inter se* the Citizens and the Government. The activity of the Government has to be such that the citizens repose faith in the Government and its activities. It is important to realize that this trust and faith cannot be demanded rather it has to be earned by the Government. The government has to be the harshest critic of scourge like corruption, waste and fraud in almost every sphere of life and human activity.

Capturing the spirit of serving the citizens with welfare, justice and growth, and to maintain parity while working towards achieving them, and to ensure that the means of inclusive progress and growth of India, at par, the Government of India has objectives of coming together towards building an Inclusive India, which is free from scourge of corruption, terrorism, poverty, communalism, casteism and filth. In order to take forward this pledge of creating a new India which is not only strong and prosperous but also all-encompassing, the Government of India has also launched "Sankalp se Siddhi" (Attainment through Resolve) Scheme, which aims at Good Governance.

In the present contemporary era, the New India Movement Scheme envisages an India which is free from poverty, corruption, terrorism, communalism, casteism and uncleanliness and aims to unite the entire nation by adopting the policy of Good Governance and most importantly employing technology with the focus objective of serving growth in all sectors of the nation, be it economic, political, social, technological, legal or environmental.

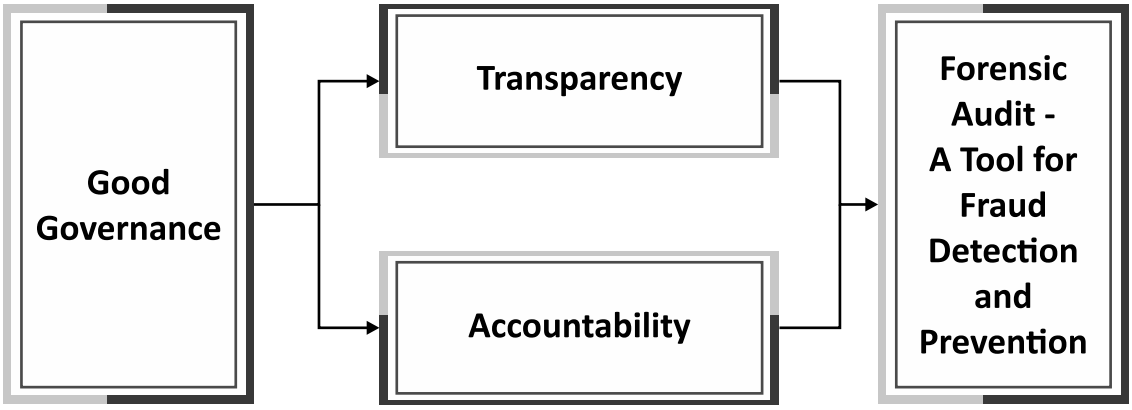
In addition to it, one should also have an insight into the Preamble of the Constitution of India, which envisages to establish a nation that provides Justice – Social, Economic and Political, along with Liberty, Equality and Fraternity to the people of India. Aligning the spirit of the Preamble of our Constitution along with the functional objectives and vision, one can say that the transformation envisaged should take place in all the spheres *i.e.* Social, Economic and Political spheres of Indian society while at the same time upholding the principles of Liberty of thought, expression, belief, faith and worship; Equality of status and of opportunity; and to promote among them all fraternity assuring the dignity of the individual and the unity and integrity of the Nation.

In this context, different measures adopted by the Government of India in the form of the reform measures like *Jan Dhan Yojna*, *National Scholarship Portal*, *Pradhan Mantri Kaushal Vikas Yojana*, *National Young Leaders Program*, *Khelo India – Boost the Sports* and many others are being brought in with the single-minded focus of transforming and reforming the nation and take it on the path of success and development. In order to transform the compassing pillars of Indian economy to enhance its performance with excellence, we are witnessing a plethora of Government initiatives including *Ease of Doing Business*, *Start-Up India*, *Stand Up India*, *Digital India* along with reformative regulating regime with the implementation of *Goods and Services Tax*, *Insolvency and Bankruptcy Code*, *Real Estate – Regulation and Development*, *Companies Amendment Act, Forensic Audit*, *Class Action Suit*, *Valuation et al.*.

A consolidated and holistic review of these reforms confirms the fact that the Government aims to establish the best practices of Good Governance wherein the virtues of Transparency and Accountability should rule the inclusive growth of our Economy as well as of Corporates in consonance. In order to serve all compassing views of growth and development of the Indian economy while making us as one of the fastest moving and emergent economies in the World, the Government of India is not only looking forward to encourage the perspectives of development, it is also introducing some strong measures by regulating the improper practices and non-compliances which hinder the way forward for the inclusive corporate culture of emergent Indian economy.

Forensic Audit: Leading way to Emergent Economy

This confirms that the Government of India is adopting a highly collaborative approach and addressing various challenges like fraud, deceit, financial misplacement and alike, which are a big hindrances in the path of inclusive growth of corporates in India.



Among other things, 'fraud' is one of the most critical ailments which not only holdups the corporate organizations where it is conducted, rather it shakes the economy of entire country which has both short term as well as long term impact.

The recent incident of financial deception faced by one of the leading Public Sector Bank of India, has not only dazed the Government, the Regulator, the Stakeholders, the Corporate community, and also the Public at large, rather it has also rung the alarm bells for all of us, specially regulators and governance professionals to critically examine the gaps responsible for making us to a witness to this kind of financial catastrophe. In fact, after making this discovery and unearthing this massive fraud which took place at PNB, the second biggest staterun lender of India, the Financial Services Secretary was constrained to direct and instruct that 'All Bad Loan Cases above INR 50 Crores at Public Sector Banks will be examined for fraud." Further the respective MDs were directed to detect bank frauds and consequential wilful default in time and refer all such cases to the CBI.

Globally, the regulators are in the best position and are the best masters to give signals of a financial cataclysm, but it seems that seldom do players heed to their conscience and follow the voice of wisdom. Keeping this vigil in mind, Forensic Audit is a dynamic approach adopted which aims to have timely detection of all frauds and also to take the requisite financial information in determining and identifying the real culprit behind the deceit.

In this whole process of timely detection of frauds and reference of such case for due investigation, Forensic Audit has an imperative role in assisting the corporates to maintain efficiency as well as merit at par. In the larger perspective, Forensic Audit is known as a tool which aims to improve the efficiency, compliance, governance and merit parameters of financial and other regulatory aspects.

Aligning the augmenting need and significance of Forensic Auditing for making sure that a company's finances are being kept safe and in order has become a growing concern in today's business environment along with the rise in money laundering and wilful default cases, the Reserve Bank of India has recently made forensic audit mandatory for large advances and restructuring of accounts.

Reserve Bank of India has recently made forensic audit mandatory for large advances and restructuring of accounts.
The Enforcement Directorate and the Serious Fraud Investigation Office have also emphasized the need for forensic audit following the rise in money laundering and Wilful default cases that are plaguing the banking system.
Regulatory Reforms for enhancing the financial stability of the country also increases the importance of Forensic Audit in the country's fight against financial offenders.

Along with Reserve Bank of India making forensic audit mandatory for large advances and re-structuring of accounts, the Enforcement Directorate and the Serious Fraud Investigation Office have also emphasized the need for forensic audit following the rise in money laundering and wilful default cases that are plaguing the banking system. They referred to the example that as the enactment of The Prohibition of Benami Property Transactions Act, 1988 increases the importance of Forensic Audit in the country's fight against financial offenders, there are other levels too, where forensic audit would prove to be a boon in settling down the principles of transparency and integrity in addition to settling down the accountability of real culprit.

The above discussion confirms that in order to assist in the paramount growth of Indian economy on the global platform under the realm of good governance, transparency, accountability and uprightness, Forensic Audit has become a need of the hour. With its key benefits in the form of Objectivity, Credibility, Expert Accounting, Enhanced effectiveness and Efficiency, Forensic Audit assures the growth of the corporates and development of the Indian Economy, which in turn leads to the inclusive growth of the emerging India. Therefore, it becomes imperative that the professionals should be well versed with basic concepts of Forensic Audit in order to effectively implementation the means and techniques of Forensic Audit towards mitigating the corporate frauds and strengthening an efficient corporate culture in India.

Further, in an era of supporting a robust economy of India, which is becoming one of the fastest emerging economies of the world, it is significant to encounter all the challenges affecting the directed growth of the economy. In such the efforts encountering the challenges, the menace of fraud, deception and scam has to be encountered at the first instance in order to promote a viable growth to corporates and economy as a whole. Considering the urgent need to check financial frauds on one side and characteristics of Forensic Audit on other side, which helps in an examination and evaluation of a firm's or individual's financial information for use as evidence in court along with a fact finding process to prosecute a party for fraud, embezzlement or other financial claims, forensic audit is leading the check in the modern day scenario.

With the contemporary phase of making a New India as free from corruption on the lines of good governance, Forensic auditing is a

- Rapidly growing area as a specialized branch of accounting and investigations; and
- Is concerned with the detection and prevention of financial fraud and white-collar criminal activities.

In this context, this book serves as a ready reference to the principles, facets and the concept of Forensic Audit, providing a basic understanding to the meaning and significance of Forensic Audit, tools and techniques of conducting it, audit and investigations as well as the laws applicable to Forensic Audit and investigations in India.

CASE STUDY

1. Inventory manipulations are some of the most common areas of fraud incidence but the auditor should look beyond a typical stock audit process.

XYZ & Co. is engaged in mining and sale of manganese ore and had availed of working capital limits from the Banks to undertake its business. The excavated ore and processed manganese were provided as collateral for the same. The company had successful business years and increased its growth plans and the corresponding working capital limits. A regulatory order banning mining activities came in to force leading to stoppage of business and a subsequent default of the lending limits. The Bank engaged forensic auditors as per the guidelines of the RBI.

Audit Approach:

- Evaluate if the business failure was genuine due to the change in regulatory regime
- Validate the business growth in the past and the justification for increased working capital limits
- Investigate the inventory control mechanisms as that forms the major collateral in this case
- Quantity and Price assumptions in arriving at inventory value as the product is a mining output with value add at various stages.

Audit Findings:

1. Poor record keeping
2. Records maintained in MS Excel
3. No proper disclosure of inventory
4. Inability to verify inventory records
5. Weak management systems.

2. Auditors should research on all group companies and related business activities of the borrower to identify potential sources of diversion of funds through purchases.

ABC & Co. is engaged in manufacturing of alloy steel with operations located in East India. The company has availed of loans for expansion of capacity in order to meet the growth plans of the company. The project cost was revised during the implementation and an additional loan was provided by the lenders. The account turned NPA before the new facility could get operational and was subject to a forensic audit as mandated by the RBI Guidelines.

Audit Approach:

- Study the techno-economic feasibility study of the project
- Identify the major procurement needs and sourcing plans as per the detailed project report (DPR)
- Understand the procurement process as defined in the management systems of the company
- Review the procurement decision related documentation – call for quotations, review mechanism, price comparisons, negotiations before awarding the contract for supply of materials and services
- Verify the documents for genuineness of the quotes received
- Contact vendors of high value items to establish if the procurement process was implemented in spirit o Identify related parties in the vendors, if any
- Review all procurement related documentation – Purchase Order, Delivery Challans, Weigh Bridge slips, taxes paid and goods received notes maintained at the company.
- Validate the veracity of the purchase documents with a special focus on duties and levies paid on the goods purchased, the transportation receipts and weigh bridge noting, etc. for any mismatch and inconsistencies
- Cross verify the transportation documents from public sources like RTO

- Check for duplicate purchase orders for the same materials and services
- Compare the landed cost of the materials and services with the current market trends and past price data for commodity items that are tracked independently
- Research and review details of other business interests of the promoters and close family members
- Verify the sources of funds for the other business interests of the promoters.

Audit Findings:

1. Errors in the purchasing process. Further company had infused funds in another project with an unrelated business interest, several transactions with related parties as suppliers of goods and services.
2. Layer of purchase transactions instead of direct purchases.
3. False quotations, duplicate purchase orders, fake transportation bills,
4. Inflated of the project cost.

LESSON ROUND-UP

- In general, Forensic Audit represents an area of finance that combines detective skills and financial acuity. Further, Forensic Auditing is used in a number of ways and for a number of purposes and not just for criminal activity detection.
- In order to catch the glimpse of Forensic Audit in totality, it also become significant to know and understand the meaning of Audit itself. As per English Oxford Dictionary, "Audit" means an official inspection of an organization's accounts, typically by an independent body. It also states a word of caution that many a times, audits are not expected to detect every fraud.
- Forensic audit is, in general, referred to as an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court.
- As per the definition given in Investopedia, Forensic Audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in court.
- Forensic audit is becoming increasingly frequent for top leadership searches as stringent corporate governance norms and increasing stakes are prompting Indian and multinational companies to make sure that the people they take on board have no blotches on their track record. In order to assist in the paramount growth of Indian economy on the global platform under the realm of good governance, transparency, accountability and uprightness, Forensic Audit has become a need of the hour.
- Forensic Auditing in general is referred as a discipline of detecting frauds in the organizations and gathering and presenting financial information in a form of evidences that will be accepted by a court of jurisprudence against perpetrators of economic crimes.
- **Forensic Audit cover areas such as:**
    i. Frauds Finding
    ii. Fraud detection and prevention techniques
    iii. Fraud related auditing

iv. Investigation and analysis of financial evidence

v. Development of computerized applications to assist in the analysis and presentation of financial evidence

vi. Communication of findings, collections of documents; and Assistance in legal proceedings.

- **Key Advantages of Forensic Audit**

i. Detection and Responsibility of Corruption

ii. Detection of Asset Misappropriation

iii. Detection of Financial Statement Fraud

iv. Fraud Identification and Prevention

v. Making Sound Investment Decisions

vi. Formulation of Economic Policies

vii. Rewarding Career Opportunity.

- **Few instances on the occurrence of which an entity should direct for Forensic Audit:**

i. Theft of business information or where business systems have been hacked,

ii. Issues identified by Whistle Blowers,

iii. Reconciliations resulted in unidentified material differences,

iv. Suspicious of fraud or illegal activity,

v. Turnover has occurred and balances are showing negative results.

- **Fundamentals of Forensic Audit involves:**

i. An audit

ii. An investigation

iii. An agreed-upon procedures engagement

iv. A proactive search for fraud.

- **Stages of Forensic Audit**

Step 1 – Accepting the Investigation

Step 2 – Planning the Investigation

Step 3 – Gathering Evidence

Step 4 – Reporting

Step 5 – Court Proceedings.

- **Fraud Triangle and Fraud Risk**

A fraud triangle is a tool used in forensic auditing that explains three interrelated elements that assist the commission of fraud- Pressure (motive), opportunity (ability to carry out the fraud) and rationalization (justification of dishonest intentions). Fraud risk is the vulnerability a company/organisation has to those who are capable of overcoming the three elements in the fraud triangle. Fraud risk assessment is the identification of fraud risks that exist in the company/organisation. The planning involves the formulation of techniques and procedures that align with the fraud risk and fraud risk management.

- **Forensic Data Analysis (FDA)**

  FDA is the technology used to conduct fraud investigations; the process by which evidence is gathered, summarized and compared with existing different sets of data. The aim here is to detect any anomalies in the data and identify the pattern of such anomalies to indicate fraudulent activity. Such an analysis requires three kinds of expertise,

  i. Data analyst to perform the technical steps and write the queries

  ii. Team member with extensive experience of the processes and internal controls in the relevant area of the investigated company

  iii. A forensic scientist who is familiar with patterns of fraudulent behaviour.

- **'Fraud',** in general, refers to a wrongful or criminal deception practiced which is intended to result in financial or personal gain to oneself and a financial or personal loss to the other.

- Explanation of Section 447 of Companies Act 2013 defines Fraud and related terms as below:

  i. 'Fraud' in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

  ii. 'Wrongful gain' means the gain by unlawful means of property to which the person gaining is not legally entitled;

  iii. 'Wrongful loss' means the loss by unlawful means of property to which the person losing is legally entitled.

- In general, fraud is an act of deliberate deception with the design of securing something by taking unfair advantage of another. It is a deception in order to gain by another's loss.

- **Elements of Fraud**

  i. False and Wilful representation or Assertion

  ii. Perpetrator of Representation

  iii. Intention to deceive

  iv. Representation must relate to a fact

  v. Active concealment of facts

  vi. Promise made without intention of performing it

  vii. Representation must have actually deceived the other party

  viii. Any other act fitted to deceive

  ix. Any such Act or omission that the law specially declares as void

  x. Wrongful Loss and Wrongful Gain is Immaterial.

TEST YOURSELF

(*These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation*)

1. What do you mean by Forensic Audit? Discuss its need and significance in detail.
2. Write down the similarities and differences between Audit and Forensic Audit.
3. What are the areas covered under Forensic Audit?
4. What are the sign to conduct Forensic Audit?
5. What are the Stages of Forensic Audit? Describe each stages in details along with example.
6. What is Fraud?
7. What are the elements of Fraud?
8. What is Fraud Triangle?
9. What are the techniques to gather evidences while conducting Forensic Audit?
10. All False Statements are not fraudulent? Narrate the statement with examples.
11. Statement need not be affirmative to be considered as Fraudulent. Illustrate with examples.

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

Audit and Investigations

Lesson 11

KEY CONCEPTS

■ Forensic Audit Thinking ■ Forensic Audit Procedures ■ Forensic Data Analysis ■ Professional Negligence ■ Investigation Mechanism ■ Fraud Triangle ■ Red Flags ■ Green Flags

Learning Objectives

To understand:

- The tools for handling Forensic Audit
- The forensic data analysis, its benefits and tools for forensic data analysis
- The role of Company Secretaries in the areas of Forensic Audit
- The procedure / steps to be followed in Investigation
- What is Fraud Triangle? How it is used as a tool for conducting forensic audit.
- What are the techniques for Gathering Evidence while conducting forensic audit.
- The steps involved in Investigation
- What is Red Flags? What are the Sign of Red Flags?
- What is Green Flags? What are the Sign of Green Flags?
- Financial Statement Analysis

Lesson Outline

TOOLS FOR HANDLING FORENSIC AUDIT

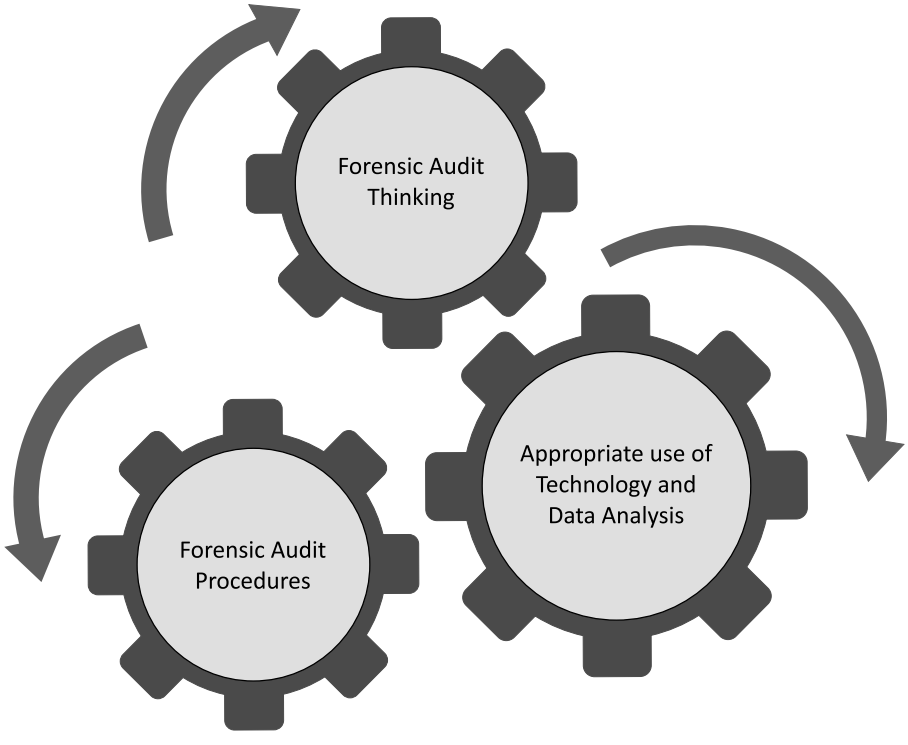
In recent years, there have been considerable changes in the business landscape. The increasing globalization, free movement of people, easy communication, technological advancements, and the shrinking of the world have helped change the business environment. These factors have led to the rapid growth of established businesses and the sprouting of new ones. However, this growth of companies has also increased in **financial crimes and frauds**.

Many businesses keep a separate department of in-house accountants who keep an eye on all the business activities and strive to minimize any irregularities in the businesses recordings. However, there are still cases of new and innovative fraudulent activities that can only be uncovered after an in-depth analysis of all the records and books of the business.

This situation has led to the growth of a niche field known as F**orensic Audit**, which can be explained as the integration of accounting and investigative skills.

Forensic procedures involve the systematic gathering of evidentiary data through the use of recognized investigative techniques that can be presented in a court of law. A forensic specialist, though not specifically defined, is an individual having expertise and/or training and experience in one or more disciplines that could be used in a forensic environment. Disciplines commonly applicable to forensic environments include accounting, auditing, fraud examination, law, computer and other technologies. Forensic accounting services generally involve the application of special skills in accounting, auditing, finance, quantitative methods, certain areas of the law and research, and investigative skills to collect, analyze, and evaluate evidential matter and to interpret and communicate findings, and may involve either an attest or consulting engagement.

Forensic Auditing is a new concept that comprises three key ingredients:



Forensic Audit Thinking (Thinking Forensically)

Involves the critical assessment throughout the audit of all evidential matter and maintaining a higher degree of professional skepticism that for example fraud or financial irregularity may have occurred, is occurring, or will

occur in the future. Furthermore, Forensic thinking is a mind shift where the auditor believes that the possibility of fraud or financial irregularity may exist and the controls may be overridden to accomplish that possibility. Forensic thinking is used throughout the audit work i.e. from start to finish.

Forensic Audit Procedures

Forensic audit procedures are more specific and geared toward detecting the possible material misstatements in financial statements resulting from fraudulent activities or error.

Audit procedures should align with Fraud Risks and Fraud Risk Assessments.

According to Donald R. Cressy, in his proposition Fraud Triangle. He highlighted that there are three interrelated elements that enable someone to commit fraud:

(a) The **Motive** that drives a person to want to commit the fraud,

(b) The **Opportunity** that enables him to commit the fraud, and

(c) The ability to **Rationalize** the fraudulent behavior.

The vulnerability that an organization has to those capable of overcoming all three elements of the fraud triangle is **fraud risk**. Fraud risk can come from sources both internal and external to the organization.

Fraud Risk Assessment: A fraud risk assessment is a powerful proactive tool in the fight against fraud for any organization. According to Association of Certified Fraud Examiners, Fraud Risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to internal and external fraud. It is important to think about a fraud risk assessment as an ongoing, continuous process, rather than just an activity. A fraud risk assessment starts with an identification and prioritization of fraud risks that exist in the organization.

Performing Forensic Procedures: Those performing forensic procedures (either the auditor or other forensic specialists like certified fraud examiners, certified financial forensics) may consider having:

- To have an investigative mindset which should be more than skeptical.
- An understanding of fraud schemes termed as occupational fraud (Corruption, Asset Misappropriation and Financial statement fraud).
- Experience in dealing with fraud issues.
- Knowledge of certain investigative, analytical, and technology-based techniques (Digital or computer forensics, e.g. how to gather, analyze and interpret data).
- Knowledge of legal processes.

Appropriate Use of Technology

Forensic Data Analysis can be used to Prevent, detect and control fraud along with other irregularities.

Forensic Data Analysis

Forensic data analysis is the process of gathering, summarizing, comparing, and aggregating existing different sets of data that organizations routinely collect in the normal course of business with the goal of detecting anomalies that are traditionally indicative of fraud or other misconduct (Donald, 2007).

Benefits of using Forensic Data Analysis

- Analyzes 100% of data sets rather than using statistical sampling—such as Risk Based Sampling.
- Can help identify potential control environment weaknesses.

- Can assist with the assessment of the effectiveness of existing anti-fraud and fraud risk management programs and practices.
- Can help to Identify potential policy and process violations—vendor acceptance/approval process, Bidding tailoring, etc.
- Can assist with interviews in investigations.

Data Analysis Tools

1. Forensic Data Analysis Process
   (i) Acquire Data and Normalize
   (ii) Brainstorming and Real-Time Data Analysis
   (iii) Output and Anomalies
2. Digital and Frequency Testing – Benford Analysis
3. Analytical Testing – Income Statement Items
4. Related Party Transaction Analysis – e-Discovery.

ROLE OF COMPANY SECRETARY AS FORENSIC AUDITOR

It is reiterated time and again that Good Governance is paramount for the inclusive growth of the country while promoting the community confidence, their participation, transparency, accountability, lead for better decisions embarking the welfare of the masses and supporting the ethical decision making, which all in consolidation call for the emergent and bright future of the nation at global platform. In the similar context, India has opted to Reform, Perform, Transform under vision New India, adhering to the best practices of good governance. In this direction, we are witnessing various legal reforms like GST, RERA, IBC, and initiation of amendments in Prevention of Money-laundering Act, 2002 and alike.

The objects of all these reforms and initiatives is to support and ensure inclusive growth and development of the nation in the all the sphere while encountering the challenging hindering the growth of those spheres.

When talking all compassing growth, economic growth is one of the significant spheres to be adhered with the premium practices of good governance and henceforth the glitches bugging the emerging growth of economy are tackled by the government at priority. In this context among other things, Corporate Frauds are considered as one of the major challenges which is obstructing the growth of corporates as well as of economy as a whole.

Right from initiating the amendments in the Prevention of Money-laundering Act, 2002 (PMLA) to enhancing the scope of preventing and punishing the frauds with the assistance of Serious Fraud Investigation Office, Government is working at length and breadth to enhance governance in the corporates and to ensure corporate compliances at par.

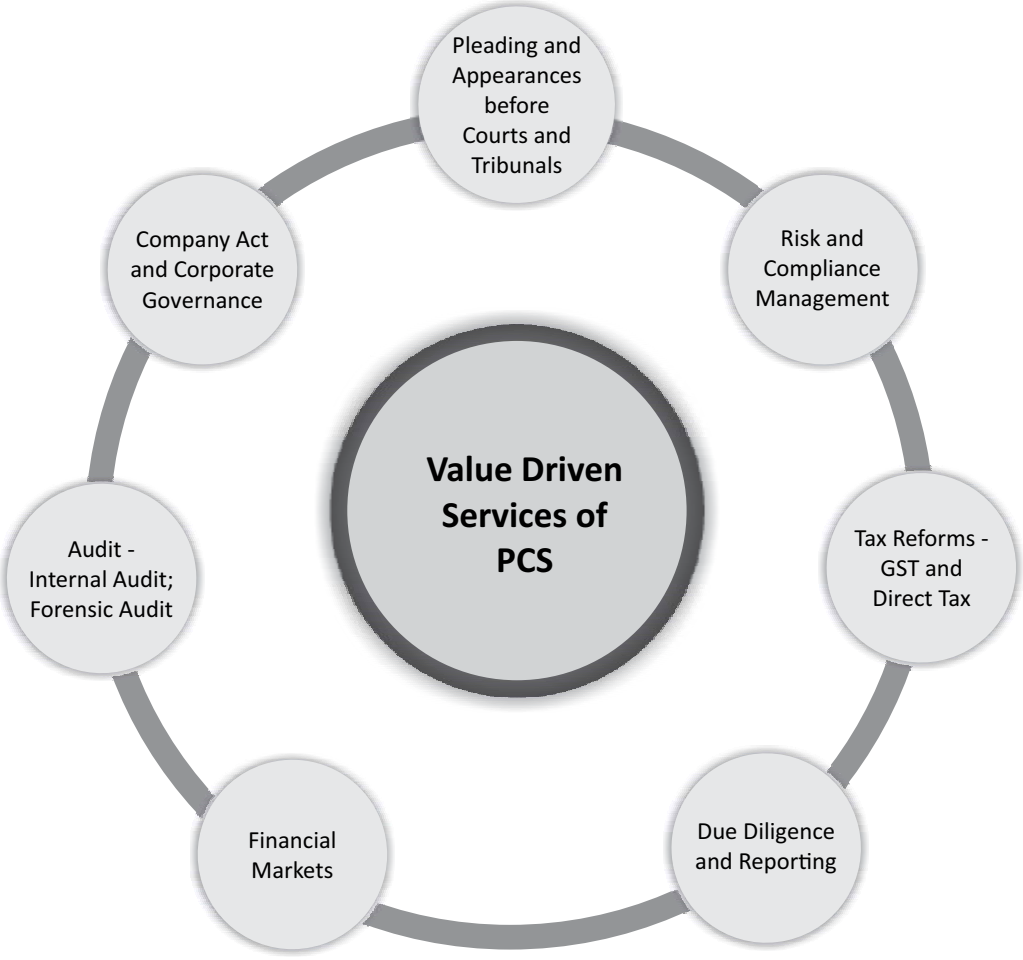
SFIO is a multi-disciplinary organization under Ministry of Corporate Affairs, consisting of experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital market and taxation for detecting and prosecuting or recommending for prosecution white-collar crimes/frauds. SFIO has head office in New Delhi and regional offices in Maharashtra, Andhra Pradesh, Tamil Nadu and West Bengal.

It should be comprehended that corporate compliance lies not in the adequacy of legislature, but in its implementation. Here comes the effective role of Company Secretaries to implement the enactments of various laws enough to eradicate fraud completely. Implementation of the law should be given more importance, to reduce the occurrence of fraud. Indeed, a directed implementation of the provisions promoting the parameters of the governance is similar to what is blood for the veins.

Under this context, one must not forget that in the last five decades, the institute of Company Secretaries of India along with its expert professional commune has immensely contributed in turning each and every stone positively sighting the successful implementation from governance to good governance and from good to now sustainable governance in our country.

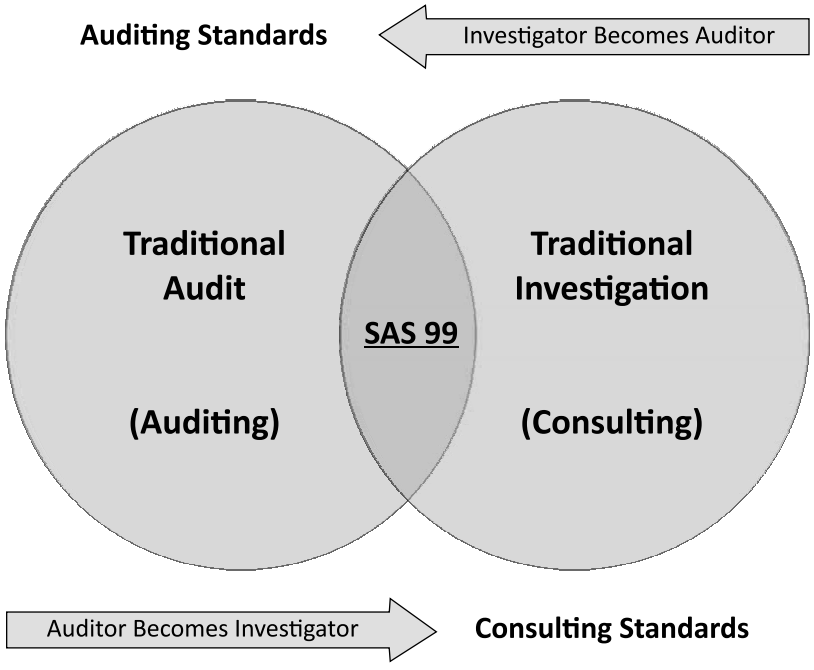
In the paraphrase of reforms, good governance, interpretation leading the world in the direction of transformation, the performance and role of Company Secretaries tends vital. In a system of reformed rules, practices, processed by which the new era of good governance is directed and subsumed, it is the Company Secretary who balances the interest of various stakeholders and ensure well complied mechanism of these reforms.

Company Secretaries decides the Corporate Culture of India and ensures in all the ways that the companies in India follow the laws and regulations, do not mishandle the accounts, and are honest in their work."



In the environment where government is directing on establishing the premium practices of governance in general and of corporate governance in specific, Company Secretaries both in practice and employment are providing their value driven professional expertise in the varied face of contemporary transformation including Financial Markets, Capital Market, Secretarial Audit, Forensic Audit, Due Diligence and Reporting, IBC, Valuation, RERA, GST, Direct Tax, Internal Audit, Risk and Compliance Management, Insolvency Professionals before NCLT and NCLAT, and many alike.

Among all, the role of company secretaries is expending in the era of forensic audit wherein they are crucially assisting in preventing, regulating and penalizing the instance of corporate frauds.



Source: Durkin Forensic Incorporated

Right from conducting forensic audit to examining the evidences, from finding the culprit behind the fraud to appearing in the court for submitted the testimony, a Company Secretary is apt in serving his professional excellence as a forensic auditor.

To summarize, where forensic audit is a detailed engagement which requires the expertise of not only accounting and auditing procedures but also expert knowledge regarding the legal framework, and a forensic auditor is required to have an understanding of various frauds that can be carried out and of how evidence needs to be collected.

In this context, Company Secretary is a Catalyst in Upholding Good Governance via Forensic Audit. His role in Specific to Forensic audit is discussed as below:

A Forensic Auditor is often retained to analyze, interpret, summarize and present complex financial and business-related issues in a manner that is both understandable and properly supported. Forensic Auditors can be engaged in Public Practice or employed by Insurance companies, banks, police forces, government agencies and other organizations. The Role of Company Secretary as a Forensic Auditor may be understood as follow:

1. **Criminal Investigations**

   A Company Secretary would use his/her investigative accounting skills to examine the documentary and other available evidence to give his/her expert opinion on the matter. Their services could also be required by Government departments, the Revenue Commissioners, the Fire Brigade, *etc*. for investigative purposes. Practicing forensic accountants could be called upon by the police to assist them in criminal investigations which could either relate to individuals or corporate bodies.

2. **Personal Injury Claims**

   Where losses arise as a result of personal injury, insurance companies sometimes seek expert opinion from a forensic auditors before deciding whether the claim is valid and how much to pay.

3. Fraud Investigations

A Company Secretary might be called upon to assist in business investigations which could involve funds tracing, asset identification and recovery, forensic intelligence gathering and due diligence review. In cases involving fraud perpetrated by an employee, the forensic auditors will be required to give his/her expert opinion about the nature and extent of fraud and the likely individual or group of individuals who have committed the crime. The forensic expert undertakes a detailed review of the available documentary evidence and forms his/ her opinion based on the information gleaned during the course of that review.

4. Investigation and Inspection

Company Secretary may help the Police, ACB and other investigating authorities in collecting evidences and other investigation purposes. For example, section 157 Cr.P.C, 1973; sections 17 and, 18 of the Prevention of Corruption Act, 1988; Section 6 of The Bankers Books Evidence Act, 1891; Section 78 of Information Technology Act, 2000; Section 447 of the Companies Act, 2013 wherein the Court or Police may require the skills of Forensic auditors while inspecting any books in so far as related to the accounts of an accused.

5. Expert Opinion

Company Secretaries see and carefully examine the accounts and balance sheets and use his skills to find out whether there is any fraud committed or any anomaly associated with it by giving his expert opinion. This finds place in for example section 45, section 118 of Indian Evidence Act, 1872; section293 of Cr.P.C, 1973.

6. Professional Negligence

The forensic auditor might be approached in a professional negligence matter to investigate whether professional negligence has taken place and to quantify the loss which has resulted from the negligence. A matter such as this could arise between any professional and their client. The professional might be an accountant, a lawyer, company secretary etc. The forensic expert uses his/her investigative skills to provide the services required for this assignment.

7. Expert Witness Cases

Company Secretary as Forensic Auditor often attend court to testify in civil and criminal court hearings, as expert witnesses. In such cases, they attend to present investigative evidence to the court so as to assist the presiding judge in deciding the outcome of the case.

8. Meditation and Arbitration

Some forensic auditors because of their specialist training they would have received in legal mediation and arbitration, have extended their forensic auditing practices to include providing Alternative Dispute Resolution (ADR) services, in absence of which a matter could be expensive and time consuming for individuals or businesses involved in commercial disputes with a third party.

9. Litigation Consultancy

Company Secretaries are eligible to be engaged in litigation and assisting with evidence, strategy and case preparation. Computer Forensics: Assisting in electronic data recovery and enforcement of IP rights etc.

10. Computer Forensics

A Company Secretary is trained in assist in electronic data recovery and enforcement of IP rights etc.

Power and Duties of Auditors and Accounting Standards

Section – 143 of Companies Act, 2013 talks about the power and duties of auditors and auditing standards. It reads: "*Every auditor of a company shall have a right of access at all times to the books of account and vouchers of the company, whether kept at the registered office of the company or at any other place and shall be entitled to require from the officers of the company such information and explanation as he may consider necessary for the performance of his duties as auditor and amongst other matters inquire into the following matters, namely: –*

a. whether loans and advances made by the company on the basis of security have been properly secured and whether the terms on which they have been made are prejudicial to the interests of the company or its members;

b. whether transactions of the company which are represented merely by book entries are prejudicial to the interests of the company;

c. where the company not being an investment company or a banking company, whether so much of the assets of the company as consist of shares, debentures and other securities have been sold at a price less than that at which they were purchased by the company;

d. whether loans and advances made by the company have been shown as deposits;

e. whether personal expenses have been charged to revenue account;

f. where it is stated in the books and documents of the company that any shares have been allotted for cash, whether cash has actually been received in respect of such allotment, and if no cash has actually been so received, whether the position as stated in the account books and the balance sheet is correct, regular and not misleading:

Provided that the auditor of a company which is a holding company shall also have the right of access to the records of all its subsidiaries and associate companies in so far as it relates to the consolidation of its financial statements with that of its subsidiaries and associate companies.

2. The auditor shall make a report to the members of the company on the accounts examined by him and on every financial statements which are required by or under this Act to be laid before the company in general meeting and the report shall after taking into account the provisions of this Act, the accounting and auditing standards and matters which are required to be included in the audit report under the provisions of this Act or any rules made there under or under any order made under sub-section (11) and to the best of his information and knowledge, the said accounts, financial statements give a true and fair view of the state of the company's affairs as at the end of its financial year and profit or loss and cash flow for the year and such other matters as may be prescribed.

3. The auditor's report shall also state –

a. whether he has sought and obtained all the information and explanations which to the best of his knowledge and belief were necessary for the purpose of his audit and if not, the details thereof and the effect of such information on the financial statements;

b. whether, in his opinion, proper books of account as required by law have been kept by the company so far as appears from his examination of those books and proper returns adequate for the purposes of his audit have been received from branches not visited by him;

c. whether the report on the accounts of any branch office of the company audited under sub-section (8) by a person other than the company's auditor has been sent to him under the proviso to that sub-section and the manner in which he has dealt with it in preparing his report;

d. whether the company's balance sheet and profit and loss account dealt with in the report are in agreement with the books of account and returns;

e. whether, in his opinion, the financial statements comply with the accounting standards;

f. the observations or comments of the auditors on financial transactions or matters which have any adverse effect on the functioning of the company;

g. whether any director is disqualified from being appointed as a director under sub-section (2) of section 164;

h. any qualification, reservation or adverse remark relating to the maintenance of accounts and other matters connected therewith;

i. whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls;

j. such other matters as may be prescribed.

4. Where any of the matters required to be included in the audit report under this section is answered in the negative or with a qualification, the report shall state the reasons therefor.

5. In the case of a Government company, the Comptroller and Auditor-General of India shall appoint the auditor under sub-section (5) or sub-section (7) of section 139 and direct such auditor the manner in which the accounts of the Government company are required to be audited and thereupon the auditor so appointed shall submit a copy of the audit report to the Comptroller and Auditor-General of India which, among other things, include the directions, if any, issued by the Comptroller and Auditor-General of India, the action taken thereon and its impact on the accounts and financial statement of the company.

6. The Comptroller and Auditor-General of India shall within sixty days from the date of receipt of the audit report under sub-section (5) have a right to, –

a. conduct a supplementary audit of the financial statement of the company by such person or persons as he may authorize in this behalf; and for the purposes of such audit, require information or additional information to be furnished to any person or persons, so authorized, on such matters, by such person or persons, and in such form, as the Comptroller and Auditor-General of India may direct; and

b. comment upon or supplement such audit report:

Provided that any comments given by the Comptroller and Auditor-General of India upon, or supplement to, the audit report shall be sent by the company to every person entitled to copies of audited financial statements under sub section (1) of section 136 and also be placed before the annual general meeting of the company at the same time and in the same manner as the audit report.

7. Without prejudice to the provisions of this Chapter, the Comptroller and Auditor- General of India may, in case of any company covered under sub-section (5) or sub-section (7) of section 139, if he considers necessary, by an order, cause test audit to be conducted of the accounts of such company and the provisions of section 19A of the Comptroller and Auditor-General's (Duties, Powers and Conditions of Service) Act, 1971, shall apply to the report of such test audit.

8. Where a company has a branch office, the accounts of that office shall be audited either by the auditor appointed for the company (herein referred to as the company's auditor) under this Act or by any other person qualified for appointment as an auditor of the company under this Act and appointed as such under section 139, or where the branch office is situated in a country outside India, the accounts of the branch office shall be audited either by the company's auditor or by an accountant or by any other person duly qualified to act as an auditor of the accounts of the branch office in accordance with the laws of that country

and the duties and powers of the company's auditor with reference to the audit of the branch and the branch auditor, if any, shall be such as may be prescribed:

Provided that the branch auditor shall prepare a report on the accounts of the branch examined by him and send it to the auditor of the company who shall deal with it in his report in such manner as he considers necessary.

9. Every auditor shall comply with the auditing standards.

10. The Central Government may prescribe the standards of auditing or any addendum thereto, as recommended by the Institute of Chartered Accountants of India, constituted under section 3 of the Chartered Accountants Act, 1949, in consultation with and after examination of the recommendations made by the National Financial Reporting Authority:

    Provided that until any auditing standards are notified, any standard or standards of auditing specified by the Institute of Chartered Accountants of India shall be deemed to be the auditing standards.

11. The Central Government may, in consultation with the National Financial Reporting Authority, by general or special order, direct, in respect of such class or description of companies, as may be specified in the order, that the auditor's report shall also include a statement on such matters as may be specified therein.

12. Notwithstanding anything contained in this section, if an auditor of a company, in the course of the performance of his duties as auditor, has reason to believe that an offence involving fraud is being or has been committed against the company by officers or employees of the company, he shall immediately report the matter to the Central Government within such time and in such manner as may be prescribed.

    Provided that in case of a fraud involving lesser than the specified amount, the auditor shall report the matter to the audit committee constituted under section 177 or to the Board in other cases within such time and in such manner as may be prescribed:

    Provided further that the companies, whose auditors have reported frauds under this sub-section to the audit committee or the Board but not reported to the Central Government, shall disclose the details about such frauds in the Board's report in such manner as may be prescribed.

13. No duty to which an auditor of a company may be subject to shall be regarded as having been contravened by reason of his reporting the matter referred to in sub-section (12) if it is done in good faith.

14. The provisions of this section shall mutatis mutandis apply to –

    a. The cost accountant in practice conducting cost audit under section 148; or

    b. The company secretary in practice conducting secretarial audit under section 204.

15. If any auditor, cost accountant or company secretary in practice do not comply with the provisions of sub-section (12), he shall

    (a) in case of a listed company, be liable to a penalty of five lakh rupees; and

    (b) in case of any other company, be liable to a penalty of one lakh rupees.

Henceforth in accordance with Section 143 the Power and Duties of a Company Secretary could be as below:

Powers of Auditor

1. ***Right to access***: Every auditor of a company shall have right to access at all time to book of accounts and vouchers of the company. The Auditor shall be entitled to require from officers of the company such information and explanation as he may consider necessary for performance of his duties. There is an inclusive list of matter for which auditor shall seek information and explanation. The list includes issues

related to: (a) Proper security for Loan and advances, (b) Transaction by book entries, (c) Sale of assets in securities in loss, (d) Loan and advances made shown as deposits, (e) Personal expenses charged to revenue account, (f) Case received for share allotted for cash. The auditor of holding company also has same rights.

2. ***Auditor to sign audit reports:*** The auditor of the company shall sign the auditor's report or sign or certify any other document of the company and financial transactions or matters, which have any adverse effect on the functioning of the company mentioned in the auditor's report shall be read before the company in general meeting and shall be open to inspection by any member of the company.

3. ***Auditor in General Meeting:*** It is a prime requirement under section 146, that the company must send all notices and communication to the auditor, relating to any general meeting, and he shall attend the meeting either through himself or through his representative, who shall also be an auditor. Such auditor must be given reasonable opportunity to speak at the meeting on any part of the business which concerns him as the auditor.

4. ***Right to remuneration:*** The remuneration of the auditor of a company shall be fixed in its general meeting or in such manner as may be determined therein. It must include the expenses, if any, incurred by the auditor in connection with the audit of the company and any facility extended to him but does not include any remuneration paid to him for any other service rendered by him at the request of the company.

5. ***Consent of auditor:*** As per Section 26, the company must mention in their prospectus the name, address and consent of the auditors of the company.

Duties of Auditors

1. **Fraud Reporting:** Among others, fraud reporting is one of the major duties of a Company Secretary in the context of forensic audit. If an auditor of a company, in the course of the performance of his duties as auditor, has reason to believe that an offence involving fraud is being or has been committed against the company by officers or employees of the company, he shall immediately report the matter to the Central Government within such time and in such manner as may be prescribed. During the Performance of his duties against Corporate Frauds, a Company Secretary should keep a pace with the following-

   A. Offence of Fraud Non-Compoundable

   As the punishment for Fraud is both imprisonment and fine, it is considered a non-compoundable offence. It shows that, the commission of Fraud has become a serious offence in the eyes of law. The Act has provided punishment for fraud under Section 447 and around 20 sections of the Act talk about fraud committed by the directors, key managerial personnel, auditors and/or officers of company. Thus, the new Act goes beyond professional liability for fraud and extends to personal liability, if a company contravenes such provisions. Here, the contravention of the provisions of the Act with an intention to deceive are also considered as fraud, to name a few acts amounting to fraud-

   - Furnishing of false information at the time of incorporation of company by promoters, first directors or any other person – Section 7(5)&(6)
   - Managing the affairs of the non-profit company fraudulently – Section 8(11)
   - Misrepresenting any material information in prospectus – Section 34
   - Inducing any person fraudulently to invest money – Section 36
   - Making of applications for acquisition of any securities in fictitious names – Section 38(1)
   - Issue of duplicate shares of company with intent to defraud or deceive – Section 46(5)

- Transfer of any shares by depository or depository participant with an intent to defraud, deceive any person – Section 56(7)
- Concealment of name or misrepresenting the amount of claim knowingly of any creditor – Section 66(10)
- Failure to repay deposit with intent to defraud depositor -Section 75(1)
- Furnishing of false statement, mutilation, destruction of secretarial documents – Section 229
- Conducting business to defraud its creditors, members or any other person – Section 213 (proviso)

B. Punishment for Fraud (section 447)

Section 447 reads that 'Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud:

Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.'

C. Punishment for False Statement (Section 448)

If in any return, report, certificate, financial statement, prospectus, statement or other document required by, or for, the purposes of any of the provisions of this Act or the rules made thereunder, any person makes a statement, –

- which is false in any material particulars, knowing it to be false; or
- which omits any material fact, knowing it to be material.

He shall be liable under section 447.

D. Punishment for False Evidence (Section 449)

If any person intentionally gives false evidence –

- upon any examination on oath or solemn affirmation; or
- in any affidavit, deposition or solemn affirmation in or about winding up of any company under this Act, or otherwise in or about any matter arising under this Act.

He shall be punishable with imprisonment for a term which shall not be less than three (03) years but which may extend to seven years (07) and with fine which may extend to ten lakh rupees (Rs. 10 Lacs).

E. Punishment where no specific penalty or punishment is provided (Section 450)

If a company or any officer of a company or any other person contravenes any of the provisions of this Act or the rules made thereunder and for which no penalty or punishment is provided elsewhere in the Act, they shall be punishable with fine which may extend to ten thousand rupees (Rs. 10,000) and where the contravention is continuing one, with a further fine which may extend to one thousand rupees (Rs. 1,000) for every day after the first during which the contravention continues.

F. Punishment in case of Repeated Default (Section 451)

If a company or an officer of a company commits an offence punishable either with fine or with imprisonment and where the same offence is committed for the second or subsequent occasions within a period of three (03) years, then, that company and every officer thereof who is in default shall be

punishable with twice the amount of fine for such offence in addition to any imprisonment provided for that offence. This section is not applicable to the offence repeated after a period of three (03) years from the commitment of first offence.

Fraud Reporting Procedure

Rule 13 of Companies (Audit and Auditors) Rules, 2014 contains the operational procedure for reporting of Fraud prescribed in Section 143(12) of the Act. If the statutory auditor detects any Fraud, it is his duty to inform the same to the Audit Committee or the Board of Directors, seeking their reply within forty-five (45) days. After receiving the aforesaid reply, he has to forward his report to the Central Government within fifteen (15) days of receipt of such reply or observations. Even in the case of no reply from the Audit Committee or the Board of Directors he has to forward his report along with his comments to the Central Government within stipulated time frame. Similar provisions of Fraud Reporting are applicable to the cost auditor and the secretarial auditor.

2. ***Make report:*** The auditor shall make a report to the members of the company on accounts examined by him on every financial statement and shall state:(a) Whether he has sought and obtained all the necessary information and explanations, (b) Whether proper books of account have been kept, (c) Whether company's balance sheet and profit and loss account are in agreement with books of accounts and returns.

3. ***Audit report of Government Company:*** The auditor of the government company will be appointed by the Comptroller and Auditor-General of India and such auditor shall act according to the directions given by them. He must submit a report to them which should include the action taken by him and impact on accounts and financial statement of the company. The Comptroller and Audit – General of India shall within 60 days of receipt of the report have right to (a) conduct a supplementary audit and (b) comment upon or supplement such audit report. The Comptroller and Audit – General of India may cause test audit to be conducted of the accounts of such company.

4. ***Liable to pay damages:*** As per section 245, the depository and members of the company have right to file an application before the tribunal if they are of the opinion that the management or conduct of the affairs of the company are being conducted in a manner prejudicial to the interests of the company. They also have right to claim damages or compensation from the auditor for any improper or misleading statement made in his audit report or for any fraudulent or unlawful conduct.

5. ***Branch Audit:*** Where a company has a branch office, the accounts of that office shall be audited either by the auditor appointed for the company, or by any other person qualified for appointment as an auditor of the company. The branch auditor shall prepare a report on the accounts of the branch examined by him and send it to the auditor of the company who shall deal with it in his report in such manner as he considers necessary.

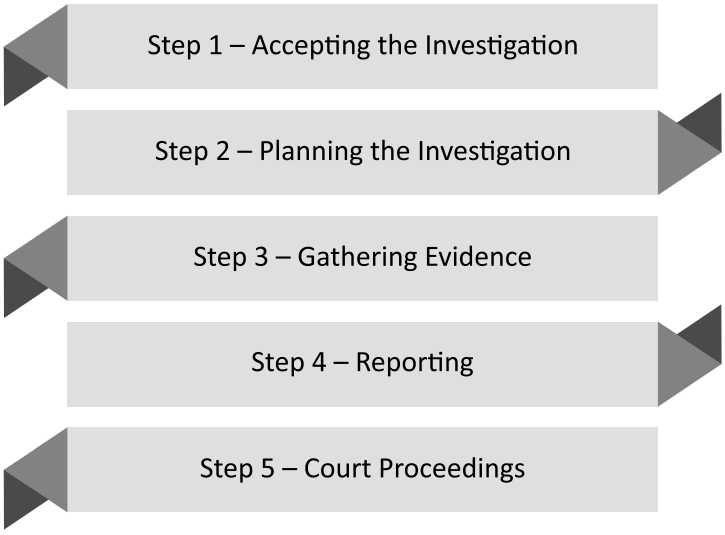
6. ***Auditing Standards:*** Every auditor shall comply with the auditing standards. The Central Government shall notify these standards in consultation with National Financial reporting Authority. The government may also notify that auditors' report shall include a statement on such matters as notified.

7. ***Winding up:*** As per section 305, at the time of voluntary winding up of a company it is a mandatory requirement that auditor should attach the copy of the audits of the company prepared by him.

INVESTIGATION MECHANISM

A forensic auditor is required to have special training in forensic audit techniques and in the legalities of accounting issues. A forensic audit has additional steps that need to be performed in addition to regular audit procedures.

Forensic Audit could be done with the adoption of the procedure detailed as below



Step 1 – Accepting the Investigation

A forensic audit is always assigned to an independent firm/group of investigators in order to conduct an unbiased and truthful audit and investigation. Thus, when such a firm receives an invitation to conduct an audit, their first step is to determine whether or not they have the necessary tools, skills and expertise to go forward with such an investigation. They need to do an assessment of their own training and knowledge of fraud detection and legal framework. Only when they are satisfied with such considerations, can they go ahead and accept the investigation.

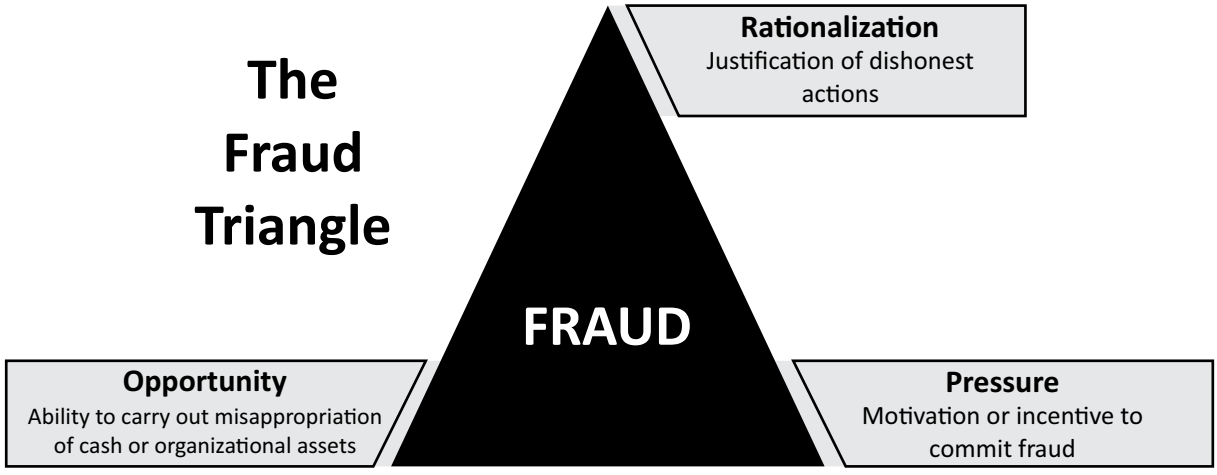
Step 2 – Planning the Investigation

Planning the investigation is the key step in a forensic audit. The auditor(s) must carefully ascertain the goal of the audit so being conducted, and to carefully determine the procedure to achieve it, through the use of effective tools and techniques. Before planning the investigation, they should be clear on the final categories of the report, which are as follows,

- Identifying the type of fraud that has been operating, how long it has been operating for, and how the fraud has been concealed.
- Identifying the fraudster(s) involved.
- Quantifying the financial loss suffered by the client.
- Gathering evidence to be used in court proceedings.
- Providing advice to prevent the recurrence of the fraud.

Fraud Triangle and Fraud Risk

A fraud triangle is a tool used in forensic auditing that explains three interrelated elements that assist the commission of fraud- Pressure (motive), opportunity (ability to carry out the fraud) and rationalization (justification of dishonest intentions). Fraud risk is the vulnerability, a company/organization has towards those who are capable of overcoming the three elements in the fraud triangle. Fraud risk assessment is the identification of fraud risks that exist in the company/organization. The planning involves the formulation of techniques and procedures that align with the fraud risk and fraud risk management.



ACFE Fraud Triangle

Planning also includes the identification of the best way/mode to gather evidence. Thus, it is necessary that ample research is done regarding certain investigative, analytical, and technology-based techniques, and also related legal process, with regard to the outcome of such investigation.

Step 3 – Gathering Evidence

In forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. In order to continue, it is pertinent that the planning stage has been thoroughly understood by the investigating team, who are skilled in collecting the necessary evidence.

The investigators can use the following techniques to gather evidence,

- Testing controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated
- Using analytical procedures to compare trends over time or to provide comparatives between different segments of the business
- Applying computer-assisted audit techniques, for example, to identify the timing and location of relevant details being altered in the computer system
- Discussions and interviews with employees
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

Forensic Data Analysis (FDA)

FDA is the technology used to conduct fraud investigations; the process by which evidence is gathered, summarized and compared with existing different sets of data. The aim here is to detect any anomalies in the data and identify the pattern of such anomalies to indicate fraudulent activity. Such an analysis requires three kinds of expertise,

- Data analyst to perform the technical steps and write the queries
- Team member with extensive experience of the processes and internal controls in the relevant area of the investigated company
- A forensic scientist who is familiar with patterns of fraudulent behavior.

Step 4 – Reporting

The reporting stage is the most obvious element in a forensic audit. After investigating and gathering evidence, the investigating team is expected to give a report of the findings of the investigation, and also the summary of the evidence and conclusion about the loss suffered due to the fraud. It should also include the plan of the fraud itself, and how it unfolded, basically the whole trail of events, and suggestions to prevent such fraud in the future.

Step 5 – Court Proceedings

The last stage expands over those audits that lead to legal proceedings. Here the auditors will give litigation support as mentioned above. The auditors are called to Court, and also included in the advocacy process. The understanding here is that they are called in because of their skill and expertise in commercial issues and their legal process. It is important that they lay down the facts and findings in an understandable and objective manner for everyone to comprehend so that the desired action can be taken up. They need to simplify the complex accounting processes and issues for others to understand the evidence and its implications.

TYPES OF INVESTIGATIONS

A fraud investigation tries to determine whether fraud has taken place and tries to detect evidence of fraud has occurred. Fraud is considered to involve misrepresentation with intent to deceive. If a company makes specific promises about a product, for example, in order to sell that product, they may be guilty of fraud if they are aware that the product does not work as advertised. Fraud is a very real and costly problem in today's world, and it causes not only loss of money but also loss of life and serious injuries. Most fraud investigations begin with a meeting between the investigator and the client. The person launching the investigation explains to their investigators why they suspect fraud has taken place and hand over any evidence they have to the investigator. A good fraud investigator will use this initial information to find more evidence and more facts. A fraud investigator may use surveillance, asset searches, background checks, employee investigations, business investigations, and other types of methods to get to the bottom of a case. In most cases, fraud investigations are investigations of white collar crime, which involves surveillance and careful consideration of complicated financial records.

The forensic auditor could be asked to investigate many different types of fraud. It is useful to categorize these investigations into following groups to provide an overview of the wide range of investigations that could be carried out. The three categories of frauds are corruption, asset misappropriation and financial statement fraud.

1. **Corruption**

   There are three types of corruption fraud: conflicts of interest, bribery, and extortion. Research shows that corruption is involved in around one third of all frauds.

   - In a conflict of interest fraud, the fraudster exerts their influence to achieve a personal gain which detrimentally affects the company. The fraudster may not benefit financially, but rather receives an undisclosed personal benefit as a result of the situation. For example, a manager may approve the expenses of an employee who is also a personal friend in order to maintain that friendship, even if the expenses are inaccurate.
   - Bribery is when money (or something else of value) is offered in order to influence a situation.
   - Extortion is the opposite of bribery, and happens when money is demanded (rather than offered) in order to secure a particular outcome.

2. **Asset Misappropriation**

   By far the most common frauds are those involving asset misappropriation, and there are many different

types of fraud which fall into this category. The common feature is the theft of cash or other assets from the company, for example:

- Cash theft – the stealing of physical cash, for example petty cash, from the premises of a company.
- Fraudulent disbursements – company funds being used to make fraudulent payments. Common examples include billing schemes, where payments are made to a fictitious supplier, and payroll schemes, where payments are made to fictitious employees (often known as 'ghost employees').
- Inventory frauds – the theft of inventory from the company.
- Misuse of assets – employees using company assets for their own personal interest.

3. Financial Statement Fraud

This is also known as fraudulent financial reporting, and is a type of fraud that causes a material misstatement in the financial statements. It can include deliberate falsification of accounting records; omission of transactions, balances or disclosures from the financial statements; or the misapplication of financial reporting standards. This is often carried out with the intention of presenting the financial statements with a particular bias, for example concealing liabilities in order to improve any analysis of liquidity and gearing.

METHODS OF INVESTIGATIONS

As appears from the previous discussions that a forensic investigation is a very specialist type of engagement, which requires highly skilled team members who have experience not only of accounting and auditing techniques, but also of the relevant legal framework.

In the forensic audit, the auditor need to ***plan the Investigation***, and with this he is required to understand what the focus of the audit is. For example, the organization might be suspicious about possible fraud in terms of quality of raw material supplied. The forensic auditor will plan their investigation to achieve objectives such as:

- Identify what fraud, if any, is being carried out
- Determine the time period during which the fraud has occurred
- Discover how the fraud was concealed
- Identify the perpetrators of the fraud
- Quantify the loss suffered due to the fraud
- Gather relevant evidence that is admissible in the court
- Suggest measures that can prevent such frauds in the company in future.

Further after understanding the possible type of fraud that has been carried out and how it has been committed, ***the auditor is required to support the evidence collected with adequacy, enough to prove the identity of the fraudster(s) in court,*** reveal the details of the fraud scheme, and document the amount of financial loss suffered and the parties affected by the fraud.

With this, Forensic auditors are required to take precautions to ensure that documents and other evidence collected are not damaged or altered by anyone. Henceforth the forensic audit need be done with specialized method of investigation so that the audit could rear the objective results.

Forensic Audit Investigation Methodology

Forensic investigation is the utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. Forensic Investigators are be grounded in accounting, medicine, engineering or some other discipline. Forensic investigation is the examination of

evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court. An example would be a Forensic Audit of sales records to determine the quantum of rent owing under a lease agreement, which is the subject of litigation.

Umeraziz (2014) while discussing the methodology to be followed by fraud/forensic auditors/investigators opines that the examination could be approached from both the angels of whether the fraud could have occurred and whether it could not have occurred. The methodology which he believes that is straight forward as follows:

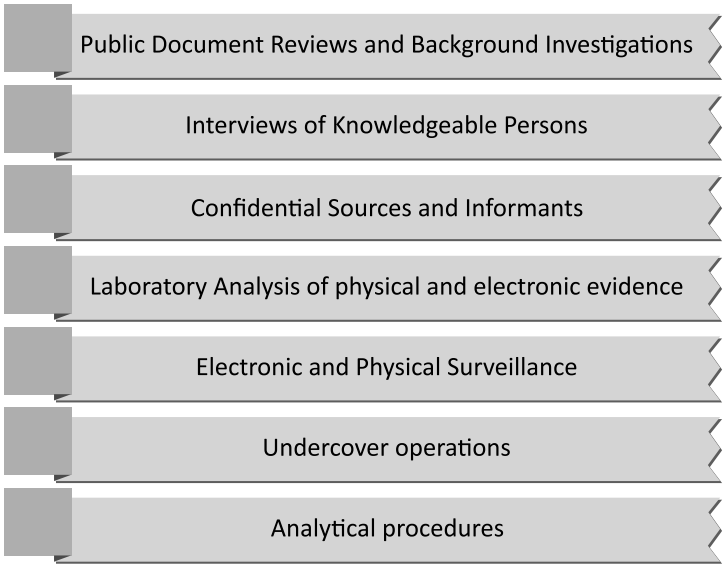
1. Analyzing data which is available
2. Creating a hypothesis based on such data
3. Testing the hypothesis
4. Refining and altering the hypothesis

Common techniques used for collecting evidence in a forensic audit include the following:

1. **Substantive Techniques** – For example, doing a reconciliation, review of documents, etc.
2. **Analytical Procedures** – Used to compare trends over a certain time period or to get comparative data from different segments
3. **Computer-Assisted Audit Techniques** – Computer software programs that can be used to identify fraud
4. **Understanding Internal Controls and Testing** them so as to understand the loopholes which allowed the fraud to be perpetrated.
5. **Interviewing and Interrogation**- Interview and Interrogation are two major techniques in investigation. That are used to elicit responses from the suspect or accused. It should however be noted that the investigator (interviewer or interrogator) cannot usurp the power of the court of competent jurisdiction by pronouncing the suspect or accused guilty. His/her role is to gather evidence that can be used to prove or disprove the act in issue (Fred, John, Joseph, Brian, 2004, Oyedokun, 2014).

Seven Investigative Tools

Further, on forensic audit procedures, there are seven recognized investigative tools and techniques used by forensic specialist / fraud examiners. (Richard 2013)



1. Public Document Reviews and Background Investigations

At the onset of an investigation, the forensic specialist may conduct or engage another specialist to conduct a background investigation of the business; its owners, employees, related parties, competitors; and any potential targets of the investigation. The process continues as new information or new individuals are identified that warrant further investigation.

A background investigation may identify current, historical, and other relevant information that may be helpful to the forensic specialist. Such information may include real and personal property records, corporate and partnership records, civil and criminal records, and stock trading activities on the part of management or board members. Through a review of publicly available records, a forensic specialist may be able to determine or understand possible motives (incentives and pressures) for perpetrating fraud. For instance, a forensic specialist may identify insider trading activities, related party transactions, or businesses owned or controlled by individuals under investigation, which could indicate a conflict of interest.

2. Interviews of Knowledgeable Persons (the witness and the accused)

The primary purpose of an interview is to gather evidence through facts and other information supplied by witnesses. Interviewing is performed throughout an investigation. With each successive interview, the forensic specialist should obtain background information about the witness, the subject matter of the investigation, and the target(s) of the investigation. As a result of the dynamic nature of the investigative process, evidence obtained from all of the investigative techniques employed can provide additional leads and areas to explore in interviews. With each successive interview, new records and additional witnesses may be identified. This progressive approach to the investigation allows peripheral witnesses to be interviewed with the purpose of having the target or targets of the investigation interviewed last.

Forensic specialists who perform attest or litigation services engagements normally do not interrogate individuals in order to obtain admissions of guilt. The primary reason forensic specialists do not normally get involved in interrogations is that legal counsel normally engages forensic specialists and controls the investigation. If a forensic specialist is working under the direction of counsel, one can argue that the target of an investigation may need to have his or her own counsel present. In addition, various legal issues may arise during the course of an interrogation that could complicate the investigation. Last, forensic specialists are fact-finders who may appear to lose their objectivity if they assume the role of interrogator seeking a confession. Although a confession may be elicited based on the evidence produced by the forensic specialist, interrogation is normally reserved for specialists such as polygraph examiners or law enforcement officers.

3. Confidential Sources and Informants

In nearly every organization, there are people who are willing to share information if they can remain anonymous. In a number of cases, confidential sources provide information through employee hotlines and anonymous letters. Additionally, former employees may provide valuable information through letters of resignation and exit interviews.

A confidential source of information may have a hidden motive for providing information. Former spouses, business partners, employees, neighbors, and friends may know specific details, but their reasons for cooperating may be suspect. The confidential source may be providing information that is intended to discredit or embarrass the target. A forensic specialist should weigh the benefit of relying on the evidence against the risk of potential damage to the case if the information is later determined to be false. A prudent forensic specialist, in the interest of exercising professional skepticism, will always attempt to corroborate the information provided by an informant or confidential source.

4. **Laboratory Analysis of physical and electronic evidence** (**Physical Forensic Analysis** which includes Handwriting analysis, fingerprint analysis, document dating, ink sampling , simulated forgery of signatures analysis, **Computer Forensics** which includes hard disk imaging, E-mail analysis, search for erased files, analyze use & possible misuse of office computers for personal use, ensure chain of custody for electronic evidence.)

   These specialists have the ability to recover previously erased electronic files and documents, and search electronic mail for evidence of fraud. Furthermore, forensic specialists have expertise in using computer technology to analyze numerous transactions, extract statistical samples, format data to apply specific investigative routines, and examine journal entries looking for signs of attempted defalcation or misrepresentation of financial statement balances.

5. **Electronic and Physical Surveillance**

   Law enforcement agencies routinely conduct physical and electronic surveillance. Private investigators and other specialists also perform these techniques under limited circumstances. A forensic specialist may recommend physical or electronic surveillance and, if appropriate, that counsel consider using one or both of the above techniques. Surveillance is primarily used to monitor people; however, the forensic specialist may turn to similar techniques for observing places or objects, such as a loading dock after business hours to determine whether inventory or equipment is being removed without authorization. The forensic specialist may also recommend that a client install surveillance cameras to protect vulnerable areas of the company, such as inventory loading and storage areas and cashier's areas.

6. **Undercover operations**

   Law enforcement agencies may use agents or officers to conduct undercover operations. Additionally, private investigators may use this technique in limited circumstances. By putting agents or private investigators in direct contact with alleged perpetrators, this technique can be an effective way to obtain first-hand knowledge of the details surrounding a fraud scheme. In most instances, forensic specialists would not participate in an undercover operation, but may recommend to the client that they consider employing this technique. Nevertheless, there have been instances in which specialists, positioned inside organizations, were able to uncover sufficient evidence of fraudulent behavior by first gaining the trust of perpetrators.

7. **Analytical procedures (Using of Ratio analysis, Trend or time series analysis, Horizontal and vertical analysis and use of work-back ratios techniques to analyze financial statement)**

   The forensic specialist's knowledge of fraud schemes and indicia of fraud is invaluable in performing analytical procedures. Forensic specialists can use a variety of analytical procedures in conducting a fraud investigation. Examples include analyzing manual journal entries for improprieties, calculating comparative ratios to analyze trends in the business, or reviewing individual or group-related transactions to check for improprieties. Also, fictitious vendors and employees can be identified, indicating that improper payments were made. Finally, investigations of sales returns and allowances can indicate the padding of sales figures.

   Reporting – A report is required so that it can be presented to a client about the fraud. The report should include the findings of the investigation, a summary of evidence, an explanation of how the fraud was perpetrated, and suggestions on how internal controls can be improved to prevent such frauds in future. The report needs to be presented to a client so that they can proceed to file a legal case if they so desire.

Finding Facts and Conducting Investigations: A Process Exemplified

International Anti-Corruption Resource Center, a Non-Profit Organization, headquartered in Washington DC has provided for some basic steps of a complex fraud and corruption investigation, that one can follow for finding facts in the case of fraud and alike.

The Basic Steps of a Complex Fraud and Corruption Investigation

The steps as provided below are generally applied to administrative investigations by international development agencies that lack law enforcement powers to compel evidence from third parties by subpoena or otherwise. Development organizations including corporates, can, however, expand their access to evidence by referring cases to law enforcement agencies for assistance, as discussed below.

(A) Preliminary Matters

Use the "Case Theory" approach to investigations

It is essential that every investigator or prosecutor develop and follow a "theory of the case" when investigating complex corruption and fraud offenses. The Case Theory approach to complex investigations is second nature to most investigators, at least the successful ones, but is misunderstood or neglected by others, with disastrous results. It is similar to the scientific method of experimentation, and involves the following steps:

- Analyze the available data to create an hypothesis;
- Test it against the available facts;
- Refine and amend it until reasonably certain conclusions can be drawn.

Expressed somewhat differently, the approach begins with an informed assumption or guess, based on the available evidence, of what the investigator thinks may have happened, which is then used to generate an investigative plan to test – prove or disprove – the assumption. It is best illustrated by example:

Example of the Case Theory Approach

Investigator One receives anonymous allegations of corruption in the award of government contracts. He pursues the case with no case theory or investigative plan. He asks a dozen witnesses if they have any knowledge of payoffs; none do (this is not unusual). He subpoenas the contract files and whatever else he can think of but sees no smoking gun as he flips through them (this is even less unusual). He confronts the suspect, who denies any wrongdoing. The investigator does not know what else to do. He has assembled a thick file and an impressive command of the contracts, but can prove nothing. Investigator Two pursues the same case, using the Case Theory approach:

- He analyzes the available data – the details of the allegations;
- Creates a simple, initial hypothesis or theory, e.g., company A is paying kickbacks to government official B for government work;
- Makes assumptions which can be used to test the theory – e.g., if the allegations are true, official B would be expected to:
  - Favor Company A in buying decisions
  - Bend or break the rules to award contract to Company A
  - Display sudden new wealth or have unexplained income.

Investigator Two uses his hypothesis to organize the investigation, i.e., looks for evidence to confirm or rebut the theory (initially, this evidence is often the "red flags" of the suspected offense.)

The Case Theory approach generates the investigative plan (see if a, b or c occurred) and if the theory is correct, evidence of guilt. If not, the investigator may amend his theory, e.g., company C is paying official A, and try again. This approach also enables one to prove, to a certain extent that a suspected act did not occur. Investigator One, after inter-viewing a dozen witnesses, did not know if bribes had been paid or not, only that he could not prove it. Investigator Two, however, can have some assurance that the alleged acts did not take place, if no evidence appears in support of his test assumptions. Remember, the Case Theory approach is simply an investigative tool to generate a hypothesis that can organize and direct an investigation, based on the information available at the time. It should not be treated as evidence itself. Do not be too committed to any particular theory and be ready to amend or abandon it as necessary.

Learn the elements of proof for the suspected offenses

Memorize the elements of proof for each of the suspected offenses, based on your theory of the case, and use them to organize the investigation and test the sufficiency of the evidence. An investigator should know at every stage of the case what evidence he needs to obtain to prove an offense. Again, many investigators neglect this fundamental rule, with the result that too little (or too much irrelevant) evidence is collected.

Carefully organize and maintain the evidence

Use charts and graphs, spreadsheets and summaries as necessary to organize and analyze complex data, but be careful not to overdo this exercise at the expense of having time to pursue leads and pursue your theory of the case. Make sure that all evidence is properly logged in, secured and accounted for, including electronic evidence, and that the source of the evidence is recorded.

Prepare the case chronology

Preparing a Chronology of Events – putting the important facts in the order they occurred – is always helpful, particularly to prove knowledge and intent and to see how a case unfolds. Concisely record the date, the event or document, and the source of information in separate columns. Include important meetings, telephone calls, email communications, travel, key documents and other potentially important events. Keep the chronology simple and focused on potentially relevant evidence – too much extraneous information will reduce its utility – and review and update it regularly. Add new information as the investigation proceeds and remove what is shown to be irrelevant.

(B) The Basic Steps of a Complex Investigation

The information below illustrates basic steps in a typical complex procurement fraud case. Most significant fraud and corruption cases occur in procurement. Ofcourse the steps are general suggestions that can be adjusted to one's situation. Some cases will require fewer steps, others perhaps more or different, such as requesting legal assistance, which is not addressed here.

The **TEN Steps** that are generally required for finding facts in a case of frauds and corruption are listed as below:

STEP ONE: Begin the case (respond to complaint, etc.)
STEP TWO: Evaluate the allegations or suspicions
STEP THREE: Conduct due diligence background checks
STEP FOUR: Complete the internal stage of the investigation
STEP FIVE: Check for predication and get organized
STEP SIX: Begin the external investigation

STEP SEVEN: Prove Illicit Payments
STEP EIGHT: Obtain the cooperation of an inside witness
STEP NINE: Interview the primary subject
STEP TEN: Prepare the final report

STEP ONE: Begin the case (respond to complaint, etc.)

If the case starts with a complaint or report, fully debrief the complainant, getting as much detail as possible. If the case starts with the discovery of a red flag, match the red flag to the potential scheme and then look for other red flags of the suspected schemes. An automated, "proactive" search for fraud indicators might be effective if the necessary data is available.

STEP TWO: Evaluate the allegations or suspicions

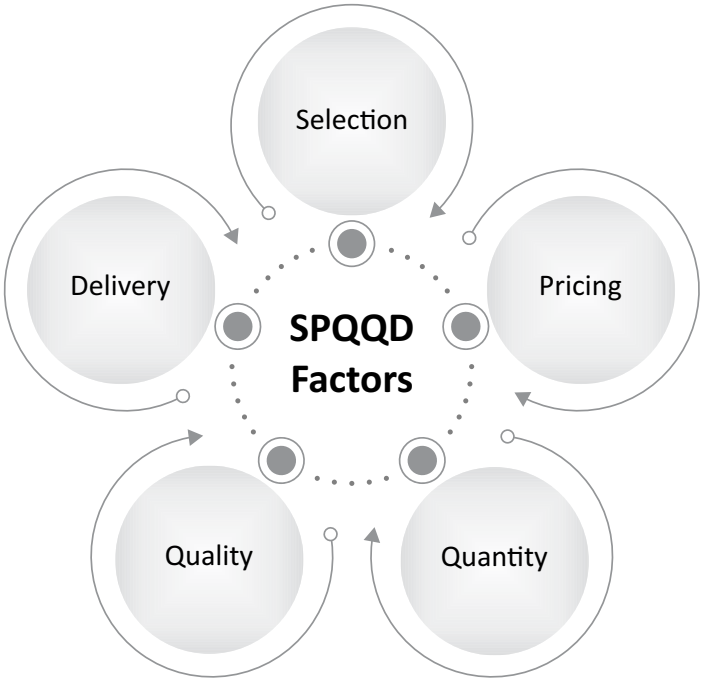
Determine whether the allegations or suspicions – the "Red Flags" – are specific and serious enough to justify an investigation, which can be time consuming, disruptive and costly.

If you determine that a complaint or report warrants further investigation, try to make a quick, preliminary assessment of the accuracy of the complaint. For example, if the complainant alleges that he or she was unfairly disqualified from a tender, examine the relevant project files to attempt to determine if this may have occurred. Use this information to prepare for the follow up interview of the complainant.

STEP THREE: Conduct due diligence background checks

Check on-line and other records on the suspect firms and individuals to evaluate the allegations and to look for other evidence of fraud or corruption, such as the presence of shell companies as subcontractors, prior debarments of a contractor or evidence that a project official is living beyond his means.

STEP FOUR: Complete the internal stage of the investigation



Complete the collection of documents, data and interviews within the investigating organization, For example:

- Look in the bidding documents for evidence of corrupt influence through the manipulation of the "SPQQD" factors – Selection, Pricing, Quantity, Quality and Delivery;
- Carefully examine bids and proposals, CVs and other documents submitted by a suspect firm for possible fraudulent representations;
- Access, with the proper authority, the relevant e-mail and computer hard drive information;
- Determine if an early interview of the subject is warranted.

STEP FIVE: Check for predication and get organized

Review the results of the investigation to date to determine if there is adequate "predication" – a sufficient factual basis – to proceed. Decide or refine the initial "Case Theory" and organize the evidence according to the elements of proof of the potential claims. If law enforcement assistance is needed (e.g., to subpoena documents, exercise search warrants or to request legal assistance) take steps to ensure that there is sufficient "probable cause" to obtain such cooperation.

STEP SIX: Begin the external investigation

Conduct interviews of witnesses outside the investigating organization, proceeding from the disinterested, cooperative witnesses to "facilitators" to co-conspirators to the subjects. Request or compel documents from third parties and the suspect contractors through negotiated agreements, the exercise of contract audit rights or, if available with law enforcement assistance, subpoenas or search warrants.

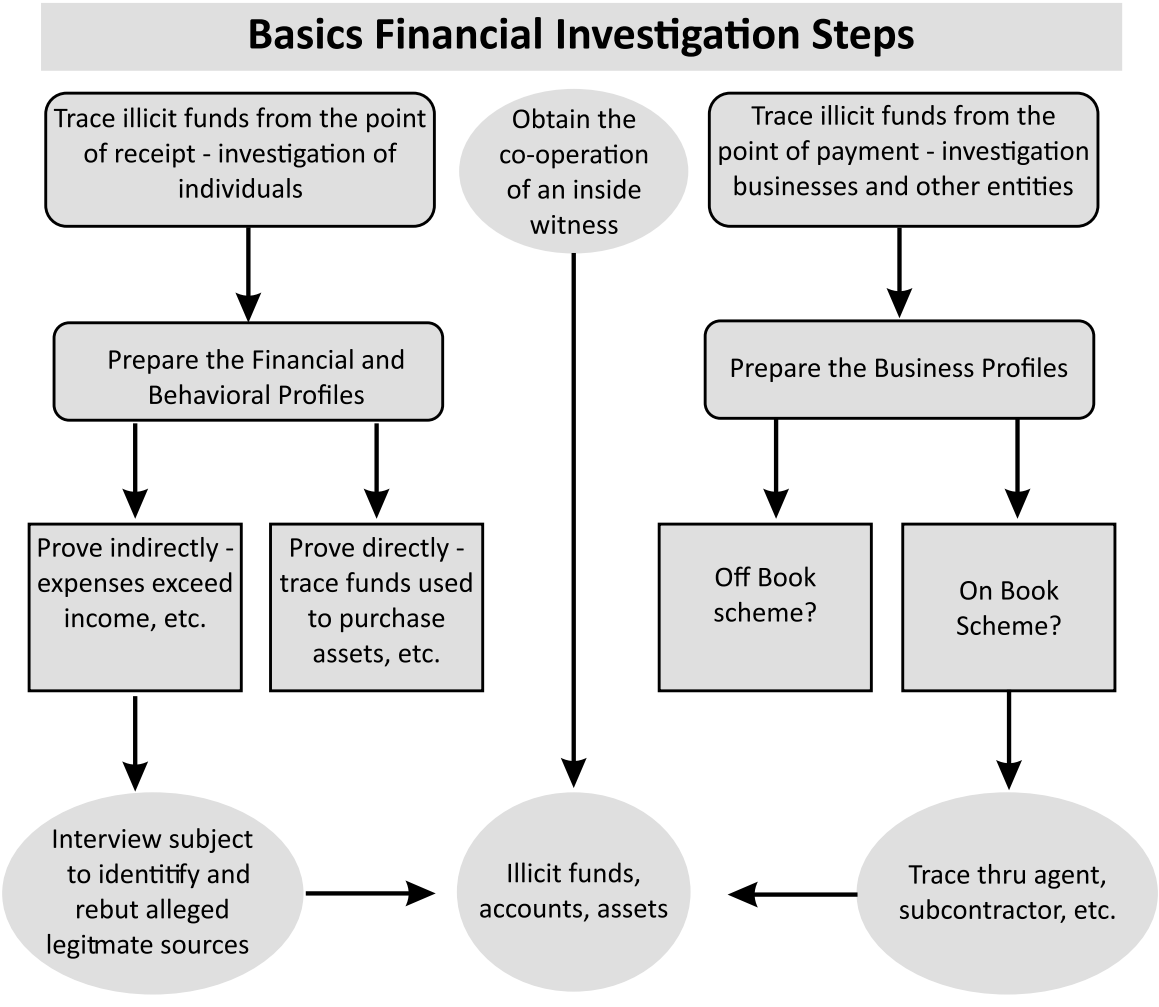
STEP SEVEN: Prove Illicit Payments

Determine the best strategy to prove illicit payments: out from the point of payment (by examining the contractor's records), or back from the point of receipt (from the suspect employee's records) and begin the tracing process. If it is not possible to prove the corrupt payments directly, try to prove them circumstantially by showing the subject displayed unexplained sudden wealth or expenditures.

The three primary ways to prove corrupt payments and fraudulent transfers are:

1. Out from the suspected point of payment, i.e., from an examination of the books, records and accounts of the entity suspected of paying bribes or making fraudulent transfers;
2. Back from the suspected point of receipt, i.e., from the accounts and financial records of the person suspected of receiving the illicit funds, or by;
3. Obtaining the cooperation of an inside witness, such as a co-conspirator, middleman or the bribe payer. This approach may be necessary to find well-hidden or laundered payments.

The three approaches are also illustrated in the chart below:



Source: International Anti-Corruption Resource Center (IACRC)

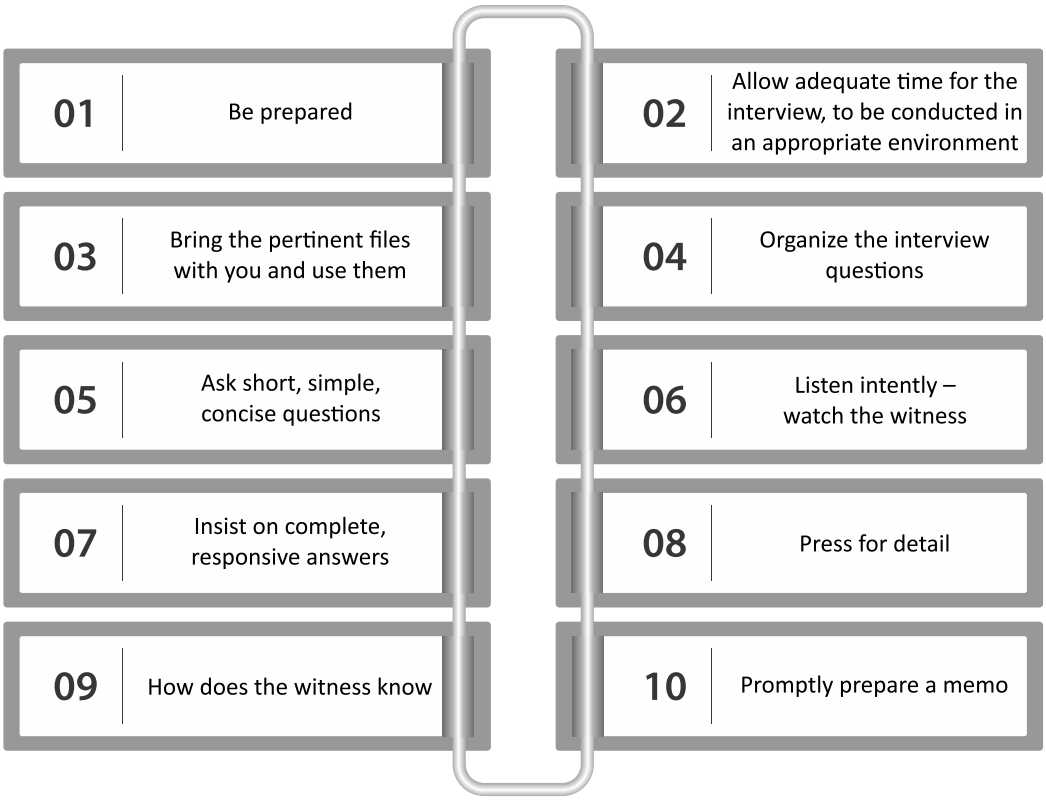
STEP EIGHT: Obtain the cooperation of an inside witness

A Cooperative Witness could be an honest inside observer or a lesser participant in the offense, such as a middleman or the smaller of several bribe payers. Decide the best strategy to obtain his or her cooperation.

Process of Interviewing a Cooperative Witness

The seemingly routine interviews in the early stages of a case are much more important, and not as easy, as they may seem. Therefore, one must organize of structure the way to interview the cooperative witness. A structured and result oriented interview would be one of the biggest strength of the Auditor in realizing rationalizing and proving the things with authentic evidences.

The Ten Most Important Points in Interviewing are listed as below:



1. **Be prepared**

   Master the known facts of the case – review the case files and prior interviews – and decide what you need from the witness to prove the offense or fill gaps. Do not rush into an interview until you are fully prepared. Prepare an outline of the points you want to cover, but do not write out the questions. That will distract you from carefully listening to the witness's answers and generating useful follow up questions. As the interview progresses, the answers will suggest the next questions.

2. **Allow adequate time for the interview, to be conducted in an appropriate environment**

   Be honest with the witness about how long the interview will take. Most interviews in complex cases take much longer than the witness anticipates. Conduct the interview in a professional environment; do not attempt to interview an important witness at lunch or in another social setting.

3. **Bring the pertinent files with you and use them**

   If the relevant files are voluminous, do the interview where the files are located. As appropriate, show the witness the relevant documents and let him or her review them before answering. Otherwise very important points will be missed or forgotten.

4. **Organize the interview questions**

   Go through the transactions in chronological order – as they occurred – or according to the documents, or in some other logical order, rather than just firing questions at random as they occur to you. If you are not organized there will be gaps in the questioning and you will inevitably forget to ask something important.

5. **Ask short, simple, concise questions**

   Avoid the long, unfocused, repetitive stream of consciousness questions that are typical of an inexperienced

or unprepared investigator. Train yourself to fully cover a particular topic by asking a series of short, simple questions. This is quite important but not easy to do. Short, clear questions make it easier for the witness to understand the question and for you to understand and evaluate the answer. And if the answers are not truthful, it will be easier to impeach the witness and rebut his or her claim that he misunderstood the question.

6. **Listen intently – watch the witness**

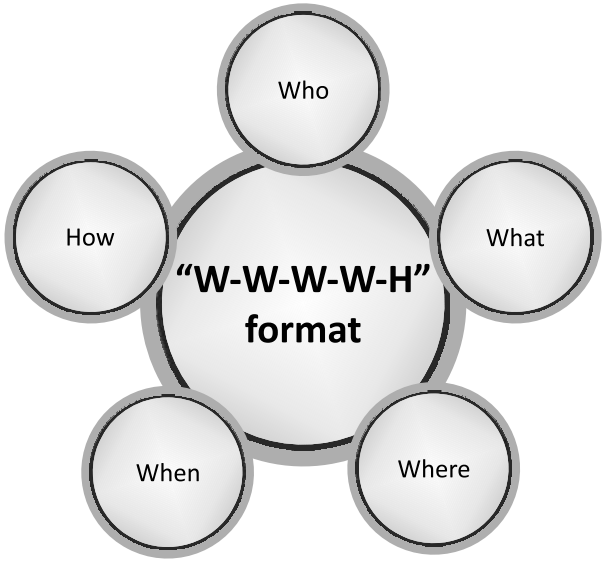
   Good interviewers rely more on their eyes and ears than their mouth in interviews. If feasible, have a second investigator attend and take notes so you can concentrate on the witness. Look at the witness (not down at your notes) as he or she answers and think about the answer – is it responsive, complete, plausible? – before asking the next question. There is no need to rush. And don't interrupt the witnesses' answer unless he or she plainly does not understand the question.

7. **Insist on complete, responsive answers**

   As noted above, listen carefully and think about the answer before asking the next question – did the witness really answer the question? Often even well-intentioned witnesses do not – keep asking until you get a proper answer.

8. **Press for detail**

   Follow the journalistic "W-W-W-W-H" format (Who, What, Where, When and How.)



   Always get the dates of key events, all the persons present at important meetings, what was actually said (as best the witness can recall, rather than just a summary of the statements) by whom, whether any record of the meetings, exist, and so on. Do not be afraid to ask the big or sensitive questions directly – ask politely, but do not beat around the bush for fear of embarrassing or upsetting the witness.

9. **How does the witness know**

   Ask, politely, how the witness became aware of the information he or she is relating. This will reveal possible unreliable hearsay – uncorroborated information from a third party – and otherwise allow you to evaluate the reliability of the information.

   Hearsay information is useful and acceptable during an investigation to generate leads and can lead to important evidence and witnesses. Eventually, however, investigators should try to obtain information from witnesses with direct knowledge of the facts. Direct knowledge means that the witness participated in the event, or observed it directly, or heard about it from the subject. The latter is known as an "admission," is not hearsay, and often is the best evidence of knowledge and intent.

10. Promptly prepare a memo

Have the witness review and correct the memo if necessary, and to sign it if circumstances suggest he or she might later recant. Delays in preparing the memo can be used to impeach its credibility. Be consistent in your practice of keeping or discarding notes. If your memos do not include everything in your notes, keep them.

The above may not be necessary if the interview is recorded, although a summary memo of the most pertinent points will be useful if the interview is a lengthy one.

Most importantly, remember that even honest, disinterested witnesses can be concerned about retaliation and the personal and business consequences of cooperation. Their decision whether to cooperate, and if so, to what extent, often depends on their assessment of the professionalism, experience and trustworthiness of the interviewer. Present yourself accordingly, in appearance, preparation, poise and interest in what the witness is relating.

STEP NINE: Interview the primary subject

In a corruption case, conduct a thorough interview of the primary subject, usually the suspected bribe recipient. Ask about his role in the suspect contract award and relevant financial issues, such as his sources of income and expenditures. Decide if there is sufficient evidence to obtain a confession; if not, try to get helpful admissions and identify possible defenses (different objectives require different tactics.) Record the interview, if possible, and request all relevant financial and other records. In a fraud case, interview the person most knowledgeable and responsible for the suspected false statement or fraudulent document. Again, decide if there is sufficient evidence to obtain a confession and, if not, try to get helpful admissions and identify possible defenses. These typically include that any false statement was an honest mistake, or that another person was responsible for a fraudulent document. Record the interview if possible.

STEP TEN: Prepare the final report

Decide what action to recommend based on the results of the investigation – an administrative sanction or criminal referral, for example – and prepare a concise final report, organized according to the elements of proof for the relevant offenses.

Note: The steps discussed above assume that the case begins with a complaint about the procurement process, without any specific information about possible illegal payments or fraud. If so, the investigation would typically begin by examining the procurement process to identify leads and eventually evidence of bribery, collusion or other wrongdoing. This is the way most such cases begin and are organized.

In other cases the investigation may begin with reports that a public official is displaying unexplained wealth or living beyond means, suggesting possible corruption, without reference to any particular procurement abuses. In that case, the forensic auditor must reverse the investigation process by first identifying the illicit financial transactions and then tracing them back to the underlying procurement transactions, if necessary.

RED FLAGS

Red flags are nothing but symptoms or indicator of situation of fraud. A red flag is a set of circumstances that are unusual in nature or vary from the normal activity. It is a signal that something is out of the ordinary and may need to be investigated further.

Definition of Red Flag for Forensic Audit

Red flags are nothing but symptoms or indicator of situation of fraud.

1. A red flag is a set of circumstances that are unusual in nature or vary from the normal activity.

2. It is a signal that something is out of the ordinary and may need to be investigated further.

Significance of Red Flags

Red Flags aids the Auditor's Responsibility to Consider Fraud & Error

1. Effective for all audits relating to accounting periods commencing on or after 1st April 2009.
2. When planning and performing audit procedures and evaluating and reporting the results thereof, the auditor should consider the risk of material misstatements in the financial statements resulting from fraud or error.
3. Two types of misstatements are relevant to the auditor's consideration of fraud:
    - Misstatements arising from misappropriation of assets.
    - Misstatements arising from fraudulent financial reporting.
4. Studies of fraud cases consistently show that red flags were present, but were either not recognized or were recognized but not acted upon by anyone.
5. Sometimes an error is just an error.

Common Types of Red flags

The most common types of Red Flags and fraudulent activity can be categorized as:

1. Employee Red Flags
2. Management Red Flags.

Employee Red Flags are like:

- Employee lifestyle changes: expensive cars, jewelry, homes, clothes
- Significant personal debt and credit problems
- Behavioral changes: these may be an indication of drugs, alcohol, gambling, or just fear of losing the job
- High employee turnover, especially in those areas which are more vulnerable to fraud
- Refusal to take vacation or sick leave
- Lack of segregation of duties in the vulnerable area

Management Red Flags are like

- Reluctance to provide information to auditors
- Managers engage in frequent disputes with auditors
- Management decisions are dominated by an individual or small group
- Managers display significant disrespect for regulatory bodies
- There is a weak internal control environment
- Accounting personnel are lax or inexperienced in their duties
- Decentralization without adequate monitoring

- Excessive number of checking accounts
- Significant downsizing in a healthy market
- Continuous rollover of loans
- Excessive number of year end transactions
- High employee turnover rate
- Unexpected overdrafts or declines in cash balances
- Refusal by company or division to use serial numbered documents (receipts)
- Compensation program that is out of proportion
- Any financial transaction that doesn't make sense - either common or business
- Service Contracts result in no product
- Photocopied or missing documents
- Frequent changes in banking accounts
- Frequent changes in external auditors
- Company assets sold under market value.

GREEN FLAGS

Above discussion on Red Flags says that red flags are symptoms or indicators of fraud, white collar crime or something detrimental to the interest of the organization. To the contrary there are other signals which could also imply the existence of fraud but do not activate alarm bells. Rather they may even lead to a greater sense of assurance and comfort in a scenario which may be potentially infused with fraud. These signals are referred as 'green flags'.

The instance of Green Flags could be helpful in identifying are unusual signs or inconsistencies, but apparently harmless or perhaps even helpful.

During the fraud detection in any organization, the auditors generally look for the red flags for indication and reduction of risk arising due the fraud for the white-collar crimes. These indicators could be shortages in stock, close nexus with third parties, missing documents, shortages in collections etc. On the contrary there could be other symptoms which leads to greater sense of assurance and comfort in a particular situation but which may potentially infuse with fraud. These signals could be termed as GREEN FLAGS. Green flags are in many ways converse to the red flags. They can also be termed as "Too Good to be True" syndrome. Few of the examples for the Green Flags could be:

- Maintenance of excess cash without any shortage
- Unexpected windfall income in certain months
- Unusually high return provided by an investment
- Company performing very well when the overall industry is in slump.

Indicators of Green Flags

1. **Excess cash reported by the cashier**: In one of the unique cases, the cashier always showed excess cash on the cash counts, but never reported any shortage of cash.
2. **Up dation of the records**: Sales and service station jobs statistically moved together in the service station and the sales outlet of a manufacturing entity.

3. **Excessive loyalty of employee:** An accountant / employee paid from his personal balances to make up for a double payment which was inadvertently approved and also paid by him.
4. **High rejection by the Quality Manager**: Rejections were made by the Quality Manager which was as high as the twice the production by the sub-contractor. The sub-contractor was penalized for the rejection of the raw material. The sub-contractor almost lost quarter of his profits for rejection.
5. **Unexpected increase of income in certain situation:** A branded educational institution received unidentified cheques for conducting specialized and popular training workshops and seminars. The cheques were received which did not contain any covering letter mentioning the purpose for which the cheques were sent.
6. **Employee making out of pocket expenses:** Employee went to outstation tour for the company purpose. As per the policy of the company, the employee did not take any advance but made expenses from his personal account. The bills for the expenses incurred were sent to the company almost after two years for reimbursement.

While conducting the audit of financial statement and fraud investigation it is imperative for the auditor to focus his attention not only for the RED Flags but also to draw his attention towards the green flags in the financial statements and the operations in the organization. Ignoring the green flags in the organization and the financial statements may be detrimental and sometimes it is possible that the green flags in the present scenario may result in converting to potential red flags.

PRACTICE MCQ

1. Management Red Flags is/are-
   a. Management decisions are dominated by an individual or small group
   b. Managers engage in frequent disputes with auditors
   c. Reluctance to provide information to auditors
   d. All of the above
2. Payment to vendors who aren't on an approved vendor list, a -
   a. Management Red flag
   b. Red flag in purchasing
   c. Red flag in payroll
   d. Red flag in account receivable
3. The Red Flag Rules apply to anyone who deals with-
   a. Financing and credit
   b. Retail merchants
   c. University healthcare practices
   d. All of above
4. Employees with duplicate social security numbers, names and addresses, a-
   a. Management Red flag
   b. Red flag in purchasing

c. Red flag in payroll

d. Red flag in cash/ account receivable

5. Which of the following is/are red flags for embezzlement:

a. Carrying usually large sum of money

b. Continuous rollover of loans

c. Significant downsizing in a healthy market

d. Photocopied or missing documents

6. _____ are those cheque tempering schemes in which an employee intercepts a company cheque intended for a third party and converts the cheque by signing the third party's name on the endorsement line of cheque.

a. Intercepted cheques

b. Altered payee schemes

c. Authorized maker scheme

d. Forged endorsement scheme

7. All of the following are indicators of financial statement fraud except:

a. Unusually rapid growth of profitability

b. Dependence on one or two products

c. Large amounts of available cash

d. Threat of a hostile takeover.

8. Which among the following will not be an example of Green flag-

a. Auditee nice behavior with auditor during audit (eg. Offering drinks during lunch)

b. Auditee is too much friendly with staff and vendors

c. Regular receipt of material of same qty

d. Employee with few or no payroll deductions

9. Jackson is a receiving clerk at a warehouse. His job is to count the number of units in incoming shipments, record the figures in receiving reports, and forward copies of the reports to the accounts payable department. One day, Jackson received a box of 20 laptop computers at the warehouse. His wife's computer just broke, so he stole one of the com

a. An asset transfer scheme

b. A purchasing and receiving scheme

c. A non-cash larceny scheme

d. None of the above

CASE STUDY

CASE STUDY 1

Jupiter Hospitals Ltd., (JHL) is a renowned corporate house owning a famous hospital called "Jupiter Hospitals". Two family groups (L and M) controlled the majority of the shareholdings in the company. The hospital is operated in Coimbatore, a non-metro city, where electronic and cheque transactions were not much high and patients mostly were making payments in cash.

The management of the company facing problems because of some disturbing events taken place during the financial year 2023-24. All these events are summarized as under:

(i) Robbery in Pharmacy :

A robbery took place in the pharmacy in the night of 29-3-2024 and cash of around Rs. 20 lakh was lost in the robbery. The robbers had entered through a window pane during 2 a.m. to 3 a.m. when none was present in the pharmacy. They decamped with all the cash in the cash chest, leaving nothing behind. No traces were found to have left behind by the robbers. Fingerprints were seen on the chest as they had not been wiped off. However, none belonged to an outsider (other than employees). The CC TV camera had turned defective a day earlier being 27-3-2024 and had been given for repairing and accordingly no help was available through CC TV recording.

Two key personnel in the pharmacy, the manager and the cashier, were supposedly doing a good job, showing remarkable growth in the night sales of the pharmacy. It is further to be noted that in nights high priced medicines were sold in huge quantities. The sales in comparison during day time was found to be less. The increase in sales was also having issues and complaints from the patients that the bills issued by the pharmacy for the goods purchased by them and cash received when asked to be verified for onward transmission for making claims, were not authenticated by saying that the same were not issued by the pharmacy. It transpired to the management that the employees involved are being in the habit of issuing the duplicate bills.

It was further reported by the internal stock auditor that there is collection of the expired goods in the pharmacy and why the same has not been got replaced or exchanged from the companies as per policy.

The police who came for investigation hence concluded that the act of robbery might have been done by a North Indian gang who were committing similar crimes in the locality and area and thus closed the case file. Insurance policy for loss of cash in safe had expired on 20-3-2024 and was not been renewed, since it was felt that no robbery would take place in a hospital which is always having movement of patients. The management entrusted the work to a forensic auditor to investigate the issue.

(ii) Related Party Transactions:

There were complaints put in the suggestion box by the various persons that some directors were making money from the purchase contracts which the hospital was entering into with the concerns in which these persons were interested. Till 15th March, 2024, the hospital had made purchases of around 22 crore from such related parties. However, on comparison with the earlier year, this was marginally higher by 5% and was thus not taken care by the management of hospital.

The allegations were that the prices paid were higher than the market prices and that some of the concerns were not reputed and have been earmarked by the drug authorities also.

There was a Purchase Committee which monitored the purchases and so the allegations were initially ignored. However, when they started pouring in, the Audit committee decided to investigate the matter and entrusted the job of ascertaining the correctness of the allegations to the forensic auditor.

(iii) Drop in Hospital Revenues:

There is an arrangement between the two groups of the shareholders that each group will administer the hospital for three years on a rotational basis. Group L's tenure had ended on 31-3-2023 and during the current year, group M had taken over the administration. Despite the number of surgeries and of other patients had not been dropped, there was a sharp fall in the revenues of hospital in the year 2023-24, except from the pharmacy. The cashier desk was managed by a director or his relative for having control over the cash. Group 'L' desires a forensic audit of the affairs to be conducted and entrusts the same to an outside forensic auditor.

In this backdrop you are being appointed as an 'Outside Forensic Auditor' to investigate all the three issues and required to give your report on the matters indicating:

(a) That it was not a robbery, but defalcation of goods camouflaged as cash sales and subsequent given shape of robbery. You are required to build up all such points from the details given on which you could have come to such conclusion. Make reasonable assumptions in this regard as being found necessary to draw up the report in the matter of robbery as reported.

(b) In respect of the related party transactions, suggest a suitable strategy to be applied to carry out the forensic audit in an effective manner.

(c) How the forensic auditor should plan his course of action to investigate and find out the cause of drop in revenue of hospital?

(d) What are the consequences under the Companies Act, 2013 and Income-tax Act, 1961 when the cause of drop in revenue is being proved?

Solution:

a) Robbery in the Hospital: Various points are being build up by the forensic auditor to prove that it was not a robbery. Those points are discussed as below:

i. The first suspicion is that no clue had been left behind by the robbers, which indicated that there is some collusion because there's nothing like a perfect robbery.

ii. The Hospital area is reasonably guarded area. Therefore it seems that it is difficult for outsiders to enter the premises and commit a robbery by breaking in some window open for making the entry.

iii. When a small cash chest is opened by fraudster using a duplicate key, it would have left some points or telltale evidence. In this perspective, it is inconceivable that there were none being found.

iv. Remarkable increase in night sales is hard to believe because in a hospital more sales take place during the day time.

v. The system login details to be seen to find out that the manager and the cashier had logged in during the night hours on the days of purported high night sales, to invoice fictitious sales.

vi. The date of robbery is few days prior to 31-3-2024, when stock taking would have been done and defalcation of stock would have been detected. To escape this, the manager and the cashier had punched in fictitious sales invoices and generate heavy cash available in the cash chest.

vii. It is worth to be noted that fraudsters had concentrated on high priced medicines, being sold in the nights –

- For making their defalcation exercise easier; and
- For generating cash balance, purported to be shown as being robbed, whereas the same was defalcated.

viii. In the cash chest, there were no fingerprints of an outsider, because no outsider was involved. A smart robber inside the organization would have wiped off all the fingerprints easily, but not an outsider. This is a case of purported employee collusion where they knew the loopholes in the internal control system which the fraudsters used to their advantage. (Internal Control System Effectiveness needs to be reviewed.)

ix. In addition to this process, the following factors needs to be looked into by the auditor for corroborating his or her investigation in the matter:

- For Manager and Cashier, it has to be checked whether a background verification done on them when they were recruited. Auditors to check that.
- How many years of service, the Manager and Cashier has rendered to the hospital.
- Were there any previous records against them?
- They also need to be interviewed to get some details about them and their personal life.
- A market intelligence team could be deployed to check on their lifestyles to see if there is a sudden change.

x. The CCTV had not turned defective by its own. This was done by the two fraudsters deliberately and not got repaired immediately, so that there is no evidence through the CCTV available for this act. Further, all the CCTV cameras needs to be checked to see if there was any trace of people entering the premises at the time of robbery.

It is further to be seen by the auditor regarding the compliant of the customers as to the issue of duplicate bills. This indicates that the low price sale had been complying in high value sales by having duplicate bills. The modus operandi in this respect needs to be looked into under the light of following perspectives:

- On what basis duplicate bills were issued.
- How many duplicate bills were issued during the month?
- Was it issued only during night sales?

The increase in the items of the dead and expired goods in the pharmacy may attract the attention of the auditors to find out the reasons. It is also possible that the employees involved had purchased such goods from the market and piled up in pharmacy so that stock inventory gets tallied on 31-03-2024.

b) Related Party Transactions: The Forensic Auditor to investigate such transactions may adopt the following strategy:

i. The register of contracts (form MBP-4) maintained under section 189 of the Companies Act, 2013 should be seen first. There is a specific query as to whether the transactions are at arm's length. The reply for the same is to be seen carefully.

ii. The Minutes of the various Board meetings in which the said Register was placed for the approval of the Board must be looked into, in order to find out the number of directors who had voted against the transactions or directors remaining neutral. The Auditor should have conducted interviews with them to ascertain their views. The reasons for voting against or remaining neutral could be crucial to the issue on hand. The remarks column, if found filled up in MBP-4, then merits special attention of the Forensic Auditor.

iii. The manner of working of the Purchases Committee must be looked into. The minutes of meetings of Purchase committee to be referred to ascertain the procedure for selection of vendors. The criteria based on which the Committee had short listed the related party concerns must be seen. Whether aspects such as qualifications, experience, etc. were met with, are to be seen. Whether competitive quotations were obtained should be seen, including the aspect of whether bids were received from other reputed companies or not. Vendor comparison sheet should be reviewed.

iv. In respect of the quotes found higher, it is essential to ascertain as to who such parties were provided with higher quote. Whether there was collusive bidding to deliberately present a higher price, so as to make the prices of related party concerns lower, should be seen. In order to find out collusive bidding, one under to undertake the following activities:

- Analyze the purchase contracts entered into in the last 5 years to comprehend since when contracts started getting awarded to related concerns.
- A disk imaging of the procurement/ committee head and his team members should be performed. The emails and other communications needs to be reviewed to identify any red flags.
- Identify vendors who have been blacklisted or discontinued in the last 5 years and contact them to understand the reason for blacklisting or discontinuation.
- Is there any conflict of interest angle needs to be checked, i.e. any relationship exists between purchase committee members and the UBOs of the companies to whom contracts were awarded?

v. Since the value of contracts with related parties exceeds Rs. 20 crores, the domestic transfer pricing provisions of the Income-tax Act, 1961 will apply and be examined in this perspective. However, for the current year, domestic transfer pricing report of an auditor may not be available; the report of the earlier years will be useful.

vi. It should be seen how the Company had treated the related party transactions in the return of income. If the company had determined the arm's length price (ALP) at lower prices and thereby voluntarily agreed for primary adjustments. This will be very good evidence to intricate collusion and loss.

vii. If any Income Tax Assessment of any earlier year in which domestic transfer pricing was involved has been concluded, the income-tax assessment order, including all assessment correspondences must be seen. Forensic auditor will get valuable information from the same.

c) Drop in Hospital Revenues

i. Major avenues from which Jupiter Hospital derives income need to be examined such as from surgery and room rent, from laboratory and Scan & X-Ray Unit and from OPD Patients.

ii. Hospital rate charts for last 3 years needs to reviewed and compared with current year to see if there is any major negative variance.

iii. The register of patients maintained at the three wings being surgical ward laboratory, scan and X – Ray and OPD must be verified. The same should be compared with the earlier year to compare the number of patients.

iv. Bank account in which payments get credited from patients' needs to be reviewed.

v. Bank and revenue account needs to be reconciled to see payment received has been completely accounted.

vi. Invoices/Bills to be reviewed to see if there are any red flags.

vii. Given that there is an increase in the number of patients opting for surgery, visiting the laboratory and using the scan facilities has not diminished, it is unlikely that there will be a reduction in the surgery fees charged (It is most likely that there will be a hike).

viii. In this scenario, the only obvious thing is that the receipts are under invoiced/ billed. Given that a director or his relative sits at the cash counter, this could easily happen.

ix. Reason for appointing a director or relative as Cashier needs to be checked.

x. Auditor should interview some patients who had recently undergone surgery, visited the lab, etc., to ascertain how much they have actually paid and what amount was stated in the receipt issued to them. Further, the auditor can interview employees or former employees so as to get some insider information.

xi. The Auditor may found that for surgeries, a mere acknowledgement was issued to patients which merely stated that they had paid the amount. There was no issue of proper receipt. Later on the receipts were prepared for lower amounts by Group M, so as to lower down the revenue and deflection of cash.

xii. For the lab, receipts issued are to be looked into as no test took place prior to the issue of the receipts.

xiii. Can arrange for some known persons to use the hospital facilities and gather live evidence as to payments and receipts issued and the modus operandi employed by the cashier.

The cumulative effect of the above leads to the inescapable conclusion, to be taken by the Forensic Auditor in his report that Group M had been suppressing the receipts of the hospital and same being drawn by them through the cashier's desk which was managed by their relative and to falsify, the drop in the revenue.

d) Consequences of the Detection of Fraud

Under the Companies Act, 2013

Considering the consequence of corporate frauds on the growth of Corporates and Economy, the Companies Act, 2013 lists down frauds and prescribe penalties and punishments for violations.

Suppressing the sales is clearly an act of fraud committed on the company. Section 447 of the Companies Act, 2013 deals with provisions relating to punishment for fraud.

The Section reads that 'Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.

The Companies Act, 2013 has provided punishment for fraud as provided under Section 447 in around 20 sections of the Act e.g. u/s 7(5), 7(6), 8(11), 34, 36, 38(1), 46(5), 56(7), 66(10), 75, 140(5), 206(4), 213, 229, 251(1), 266(1), 339(3), 448 etc. for directors, key managerial personnel, auditors and/or officers of company.

Under the Income - Tax Act, 1961

- Suppression of revenues will result in concealment of income by way of under reporting and negative reporting of the income.
- Concealment will lead to levy of penalty u/s 270 of the Income Tax, 1961, which may be of 300% of the tax on such income.
- Prosecution may also be launched on all the officers involved.

CASE STUDY 2

Thrivikram Dazzlers (TD) is a reputed diamond jewellery merchants in existence for the past two decades. Their jewellery store was located at Chennai and the branch was also operated at Mumbai.

TD had been regularly dealing with a client at Delhi named Sunil Raina & Co., (SR). SR generally electronically transfers funds to TD for purchases. An employee "EM" of them then would visit TD and take delivery of the jewellery ordered. EM had become familiar to TD, having been visiting the shop for the last three years regularly. On 24-3-2024, there was an electronic transfer of funds from SR for a sum of Rs. 16 lakhs. EM produced a letter in the company's letter head which stated that the articles purchased were gifts for special clients for certain services rendered and hence requested that invoice be made out in the name of EM for 3 necklaces and that the delivery be effected to EM.

TD mailed to SR and asked for a confirmation regarding supply of goods in the name of EM. A mail was received in reply confirming the same. TD hence complied with the same after receipt of mail from SR.

(a) On 30-3-2024, TD received a phone call from SR asking them why the goods had not yet been delivered despite the payment being made on 24-3-2024. Only then it transpired that EM had defrauded SR and TD.

Both TD and SR approach you, a leading forensic auditor, to conduct a joint forensic audit and submit a report. Both are willing to cooperate with you in providing details and information and records.

(a) Outline the aspects to be considered of the transaction by the Forensic Auditor for taking course of action in detecting the truth of the employee EM.

(b) What would have been the course of action, taken by the Forensic Auditor, in case TD is a dealer in consumer products like costly refrigerators, TV sets, etc., and the goods delivered to EM were six costly TV sets?

Solution:

a) Defalcation by employee of customer Sunil Raina & Co., Delhi

Following aspects are to be looked into by the forensic auditor for taking his course of action in detecting the truth.

i. TD and SR should be asked to lodge a complaint with police about the incident taken place of taking delivery of goods by EM from TD by having invoice being made in his name.

ii. The employment records of EM available with SR should be seen and must be looked into by whom he was referred for employment.

iii. EM's immediate reporting manager needs to be interviewed to understand EM's general conducts during his employment and if there were any issues against him. In order to understand his general conduct, following concerns must be looked into:

- Did EM keep his Manager in loop when conducting company related transactions?
- EM's residence needs to be visited to interview few people staying in that area if they know him and his family and their social image.

iv. His previous employment certificate should also be verified so as to analyze his conduct.

v. Enquiries should be made to ascertain the service records with the earlier employees of EM in a secret way. It is possible that the earlier employer certificate given by EM to SR is a fake document.

vi. If the employer really existed, then it should be investigated whether EM had any history of proved or unproved allegations against him during his employment and why he had left the job.

vii. If the previous employer had not given a clean chit to the auditor then find as how the Human Resource Department of SR had hired him. There could be a collusion here with the HR.

viii. The authorization letter in SR's letter head should be deeply looked into to find out that whether it is in legitimate company stationery or not? If yes, then a deeper scrutiny of the trial to find out as how EM could get hold of the same, should be investigated. Who signed the same must be seen and authenticity of signature of the person to be verified. If someone other than EM (forged), then here is an accomplice, which should be brought out of records.

ix. TD sent a mail to SR asking for confirmation of delivery of goods to EM. This shows that a reasonable precaution was taken by TD prior to supply. Forensic Auditor should find out whether TD send such mail to the official email id of SR or to some other email id mentioned in the "authorization letter" produced by EM. If it is an official email id, then TD is not at fault. If it was be the latter, then it could be a case of sheer negligence on the part of TD, or there could be an accomplice for EM in TD shop. These aspects merit attention and deeper scrutiny.

x. If TD had sent the mail to SR to the official mail id and got back a confirmation mail, who sent it must be investigated. This person is clearly an accomplice of EM. In case of common id, IP address of device from where it is sent to be identified.

xi. If this employee gave confirmation based on a superior's order, then it is SR which is at fault. In such cases, any act done by any of its employee (EM) will be construed to be act done by an agent, which is binding on the principal SR. TD cannot be held liable in such a situation.

xii. Checking mobile call logs to ascertain whether he has contacted any other employee in either of the companies.

The Forensic Auditor by applying the aforesaid course of action can find out the truth of the case for making out a report for TD and SR.

b) Where the goods delivered were costly TV sets instead of Jewelry

In such case, apart from the course of action as stated above, the forensic auditor should also look into the following aspects:

i. How the delivery of goods were taken of?

ii. Was it in TD's vehicle or was it arranged by EM?

iii. If TD's vehicle, place of delivery is easy to track, if latter, the vehicle owner should be found out and place of delivery be ascertained the said place can be visited to find out if there is a nearby market for such goods.

iv. E-way Bills are required under GST law for transportation, since the value of the products exceed Rs 50,000. The e-way bills should also be studied for clues, if any.

CASE STUDY 3

PQR & company are the manufacturers of sophisticated consumer products. They have a system of getting certain work done by Job Workers. The costly raw material will be sent to the Job Worker through the company's transport and delivery challan will be prepared by the Stock Manager and acknowledgement obtained from the Job-workers on delivery. Job Worker will process the material as per the company's instruction and specification and the same will be inspected by the Quality Controller of the company at the premises of the Job Worker; entire quantity of material sent earlier now in semi-finished form will be returned to the company for which the company itself provides their own transport. A reasonable percentage for shortage and wastage and rejections of a maximum of 2% was allowed by the company to the Job Worker. This engagement was established for some years and was found to be working well. Processing charges are paid to the Job Workers on receipt of the processed material along with his challan. However, some complaints have come recently from some sources that some processed materials was selling in the market.

Management is desirous of conducting a Forensic Audit. In the background of aforesaid facts, you are required to:

(a) Indicate your line of Investigation.

(b) Do the facts fall to be considered as fraud as per section 447 of the Companies Act, 2013? Discuss.

Solution:

(a) On going through the case, certain points arise viz. materials sent to job worker are costly and the company itself sends through its transport and brings back by their own transport and returned materials are accounted after deduction at 2% for wastages. It is said that it is their practice.

As an auditor, we planned to have a casual discussion with the Stock Manager on the arrangement that is going on. He explained raw material being costly, it is transported to job worker considering the safety and that after approving the process, the same is brought back by the company itself by certain authorised transporters for safety purpose. On the challan prepared by Job worker while sending back the stock, he clarified that since other document prepared by the Quality controller after allowing 2% for wastage will be accounted as usual and challan of job worker will not be considered. Regarding the wastage, he said that much importance is not given to small things.

We have decided to visit the place where the Job Work process is carried out to know the operation. He is doing the job for PQR Company only. On wastage and rejection, he said that earlier job was carried manually and some wastage or rejection had arisen but now the job is done by latest technology and very rarely wastage or rejection occurs. Now it is clear that there is no wastage and that the entire quantity was going back and therefore a deduction of 2% was unwarranted. To tackle the situation, we have taken the address of the transporters who bring back the materials.

Questioning them and investigating further, the driver of the vehicle admitted that on instruction of stock manager, every time some quantity of the processed material was under dispatch from the Job worker to the factory, a part of it would be unloaded in the premises of the stock manager and the balance alone will be delivered in the office.

With the facts ascertained, the Stock Manager was cornered who accepted that unknown to the management, he was selling the processed material and pocketing money.

The Forensic Auditor has finally unearthed the fraud for management to take action.

(b) Fraud as per Section 447 of the Companies Act, 2013 is defined as below:

i. In relation to affairs of a company or a body corporate, includes any act, any omission, concealment of any fact or abuse of position.

ii. Committed by a person or any other person with the connivance in any manner with intent to deceive, to gain undue advantage from, or to injure the interests of the company or its shareholders or its creditors or any other person.

iii. Whether or not there is any wrongful gain, or any wrongful loss.

On the strength of the facts found in this case, fraud u/s 447 of the Companies Act, 2013 is established.

CASE STUDY 4

Raj & Company has been dealing with reputed company's TVs. They are the agents of many company's TVs. They offer instalment systems payments which attracts customers and their turnover has been improving. They have a spacious office where TVs are displayed which naturally tempts the customers to visit and buy. Adjacent to their office they have taken a warehouse to keep stock of TVs received from companies and would draw stocks from the warehouse as and when required. They maintain necessary records like goods received report, sales register and stock statement on daily basis. They have the system of maintaining parallel stock ledger at the office also. There was an outbreak of fire in the warehouse and stocks and records have been completely destroyed. Raj & Company preferred their claim with the underwriters for Rs. 15 lakh being the cost of 50 TVs, which seems to be very high according to Insurance Company. Insurance Company is of the view that the claim requires to be probed before accepting.

They doubt that there is a possibility of manipulation in the claim. If you are appointed as Forensic Auditor What investigation would you follow to detect the genuineness of the claim?

Solution:

The Insurance Company has handed over to us to audit the claim preferred by Raj & Co. All records are completely destroyed along with TVs. The only material available was the parallel stock ledger at the office. After ascertaining the details of their business, we started gathering the information of quantity purchased during the past six months and the sales effected.

On going through the records of parallel register, it is observed that average sale of TVs during the past six months was 20 numbers and the purchases also an average of 20 to 25 numbers. The credit period allowed by the supplier was 30 days and customers are paying through installment and it is also seen cash sales. Raj & Co. says there is a sales drive to earn incentive and sometime they purchase increased quantity and stock in the warehouse so that they do not enter into a stock out situation and therefore, they stock in the warehouse more than 50 TVs.

On going through purchase details and sales pattern, bulk purchase of 40 or 50 numbers had not taken place but still their contention is that they had 50 TVs in the warehouse on the day of the outbreak of fire. Not being satisfied with their explanation, we have decided to inspect the warehouse. It is a small warehouse and considering the size of TV boxes, stacking norm permitted is only three boxes in a column and vacant space needed for human movement. Taking into consideration the storage volume for each model and the space required, they can store the warehouse only 8 columns and the number of TVs cannot exceed at best 24 numbers. When these queries were put up, they were shocked and accepted to reduce the claim unconditionally. It is now left to accept the claim or not since claim was inflated.

CASE STUDY 5

A bank suspects that the stock statements furnished for the 12 months during the FY 2023-24 by Ravana Handlooms, one of its borrowers, do not reflect the true position and that they have been systematically furnishing statements showing higher quantities of various items of stock as compared to the actual quantity present in their godowns, and also that the values have been overstated. The borrower is a registered supplier under the GST law. Their turnover for the year ended 31st March, 2024 is Rs. 3.4 crores and they have filed their return of income on 12th October, 2024.

As a forensic auditor appointed by the bank, how will you go about gathering evidence and what are the documents, statements, returns, etc., you will go through to check the veracity of the stock statements furnished by the borrower?

Solution:

Gathering of Audit Evidence

In forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. In order to continue, it is pertinent that the planning stage has been thoroughly understood by the investigating team, who are skilled in collecting the necessary evidence.

The investigators can use the following techniques to gather evidence:

- Testing controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated.
- Using analytical procedures to compare trends over time or to provide comparatives between different segments of the business.
- Applying computer-assisted audit techniques, for example, to identify the timing and location of relevant details being altered in the computer system.
- Discussions and interviews with employees.

- Substantive technique such as reconciliations, cash counts and review of documentation.

Documents / Papers etc., to be seen by Forensic Auditor

The Forensic Auditor should verify the following statements/papers/ documents:

1. Analyse the stock held on various dates during the FY 2023-24 and FY 2022-23. The stock statements submitted to the bank themselves may be seen in this regard.
2. Trend analysis of the two years may be carried out from above.
3. The borrower has filed the Income tax return for the AY 2024-25. Since its turnover exceeds Rs. 2 crores, it will be subject to tax audit. Form 3CD should be verified to see the comments of the auditor about valuation of stock. In case, there is any adverse comment or qualification, this will be helpful for further probe.
4. Form 3CD also furnishes quantitative details of stock, which are to be verified by the forensic auditor.
5. Forensic auditor should check whether the quantity as well as value as furnished to the banker tally with those disclosed in the Income-tax return. In case the difference is material, the same justifies strong further action.
6. GST returns filed for each month may be verified. Thus will give an idea of the selling prices of the borrower for various items. By deducting rough Gross Profit margin, the cost of goods sold can be ascertained. The Forensic Auditor can compare the said rates with the rates adopted by the borrower in the Stock statements of various months.
7. Forensic Auditor could conduct a surprise visit of the godown where the stocks are held and undertake a stock verification.

CASE STUDY 6

Vishnu Mobiles Ltd., is a domestic company dealing in mobiles of famous international brands. During August, 2023, the company suspects that its sales volume has come down, thanks to the red flag raised by the Sales Manager. Two persons L and M are handling sales of two famous brands viz., Orange (Costly mobiles) and Bamfung (economy model mobiles). Anonymous letters have come to the company about sudden spurt in the lifestyles of L and M. The company, suspecting acts of collusion and corruption, entrusts the job to you as forensic auditor. What are the types of corruption you will look for?

What will be your course of action as forensic auditor to unearth the misdeeds, if any, committed against the company?

Solution:

Forensic Audit of Corruption Fraud

There are three types of Corruption Fraud: Conflicts of Interest, Bribery, and Extortion. Research shows that corruption is involved in around one third of all frauds.

- In a conflict of interest fraud, the fraudster exerts the influence to achieve a personal gain which detrimentally affects the company. The fraudster may not benefit financially, but rather receives an undisclosed personal benefit as a result of the situation. For example, a manager may approve the expenses of an employee who is also a personal friend in order to maintain that friendship, even if the expenses are inaccurate.

- Bribery is when money (or something else of value) is offered in order to influence a situation.
- Extortion is the opposite of bribery, and happens when money is demanded (rather than offered) in order to secure a particular outcome.

Methodology to be adopted

The following methodology may be adopted by the Forensic Auditor, singly or in combination:

i. Conducting interviews with the employees of the company, especially in the sales division.

ii. Encourage the employees to post their views about L and M, in suggestion boxes anonymously kept in this regard.

iii. Where the company policy permits, check the email history of L and M for the past one year.

iv. Buyers of the two mobile products are to be interviewed to ascertain whether there is any collusion between any of them and L (or M).

v. Forensic auditor may obtain SOP for sake for these two mobiles and check whether they have been adhered to by L and M.

vi. It is possible that L and M have colluded with each other, along with some buyer. Costly products of Orange might have been billed as the other product.

vii. Confirmation of balances should be obtained from various buyers and cross checked with company records.

viii. GST returns for the month should be scrupulously checked and any fraud pattern visible therein must be looked into.

ix. Look for red flags. Were L and M too sincere in their work, without even taking sick leave or going for vacation, even though they were entitled to?

x. Market Intelligence techniques can be adopted wherein cover agent will visit the suspected person's residence area to get an understanding his lifestyle, discreetly enquire about him with the few people in the area adjoining etc.

CASE STUDY 7

Department of Foreign Trade (DFT) have received complaints from several quarters about one exporter who is alleged to have indulged in book exports (actual exports have not taken place, only the books show as if exports have taken place), against one Duryodhana Jewellers, Surat (DJS).

DFT appointed a forensic auditor (FA) to probe into the matter. The FA came out with a report proving that the complaints received were true. Discuss how the FA would have gone about in the course of his audit to prove the misdeeds of DJS.

Solution:

Forensic Audit of alleged book exports fraud

The Forensic Auditor (FA) will go about examining various aspects connected with the alleged exports of Duryodhana Jewellers, Surat (DJS). Various aspects the Forensic Auditor would have looked into, the documents and records which the Forensic Auditor would have verified and related aspects involved are as under:

a) Compare the track record of DJS for the past 5 years to see whether there is any alarming increase in the quantum of exports during the current year, as compared to the earlier / previous years.

b) Verify the details of the alleged buyers for the exported product, to see whether such buyers are located in notified jurisdictional areas for Income tax purposes. In case there are notified jurisdictional areas buyers, deeper scrutiny is required.

c) Bank records are to be thoroughly scrutinised to see whether there are actual remittances in foreign exchange from the alleged buyers.

d) Investigate the origin and the manner of utilisation of the alleged remittances received from abroad for the exports. This will help to see whether the same are funnelled out of India for remittances again into India.

e) Compare the rates shown in the various export invoices with the rates of sellers of similar products who also export.

f) Production /stock records of DJS to be seen to examine the flow of production. Sales is possible only if stock is held and stock can arise only of they are produced or purchased.

g) In case the inflow of stock is due to purchases, all the purchase invoices are to be verified.

h) Related party transactions, if any, should be looked into and in case of any, deeper scrutiny is required.

i) Form 3CD to be verified to look into transactions with related parties or with persons specified in section 40A (2) of the Income-tax Act, 1961.

j) GST returns to be checked thoroughly to see how DJS has claimed the refund for GST paid on exports.

FINANCIAL STATEMENT ANALYSIS

Financial statement analysis (or financial analysis) is the process of reviewing and analyzing a company's financial statements to make better economic decisions to earn income in future. These statements include the income statement, balance sheet, statement of cash flows, notes to accounts and a statement of changes in equity (if applicable). Financial statement analysis is a method or process involving specific techniques for evaluating risks, performance, financial health, and future prospects of an organization.

It is used by a variety of stakeholders, such as credit and equity investors, the government, the public, and decision-makers within the organization. These stakeholders have different interests and apply a variety of different techniques to meet their needs. For example, equity investors are interested in the long-term earnings power of the organization and perhaps the sustainability and growth of dividend payments. Creditors want to ensure the interest and principal is paid on the organizations debt securities (e.g., bonds) when due.

There are three major financial statements: the balance sheet, profit-and-loss statement and cash-flow statement. The balance sheet tells you about the assets and liabilities of a company. The profit-and-loss statement tells you about a company's profitability and the cash-flow statement is about the flow of cash into and out of a company.

Balance sheet: The balance sheet shows the assets that a business owns, the liabilities that it owes and the funds contributed by its shareholders.

Assets = Liabilities + Owners' equity.

Assets include land, equipment, inventory, goodwill, patents, brand value, etc. Liabilities include debt (long-term and short-term) and any other payables that a business has. Shareholder funds are in the form of equity and reserves.

A weak balance sheet is one that is saddled with debt. When a business has a strong balance sheet, it has more assets and equity than liabilities. In order to know the balance-sheet strength, can look at the debt-equity ratio.

Profit and loss Statement: As its name suggests, the P&L statement tells about the profitability of a company. The simple formula to calculate profits is Profit (loss) = Revenue - Expenses.

The head 'revenue' generally has two entries: revenue from sales and other income. Other income is the revenue from sources other than the core area of the company's operations. For instance, it could be income from investments, dividends, royalties, etc.

The head 'expenses' constitutes the categories of expenditure such as cost of raw materials, employee costs, etc. On subtracting the total costs from the total revenues, we get the 'operating profit', which is nothing but a company's profit from its core operations.

In order to arrive at the final profit figure, any miscellaneous income or loss is to be added to or subtracted from the operating profit. Finally, net profit is obtained after deducting the tax applicable.

Cash-flow statement

The cash-flow statement shows the movement of cash in a business. While businesses can misstate their profits through accounting jugglery, they can't fudge the movement of cash. Hence, a cash-flow statement provides a true picture of a company's financial health. However, for banks and finance companies, the cash-flow statement is of limited use as they follow a different business model than other types of businesses.

The cash-flow statement has three components: cash flows from operating activities, from financing activities and from investing activities. The statement also mentions the current cash holding of the business.

What need to check in the data is whether flows from operating activities are positive or not. If they are positive, it means that the company is able to generate cash from its operations. If they are negative, it means that the company is losing money. While it may show profits in its P&L statement, negative flows from operations should ring an alarm.

Cash flows from financing activities show the money raised for the company's operations or the money paid towards debt repayment. The former will be a positive number on the statement, while the latter will be a negative number.

Cash flows from investing activities capture the cash used in investments. For instance, a business that has generated surplus cash may park it in a bank fixed deposit. Next year it may withdraw cash from that FD. The former will be a negative number on the statement, while the latter will be a positive number.

The balance sheet, profit-and-loss statement, as well as the cash-flow statement contain the data necessary to guide investors looking to invest in a company. Ratios used in analysing stocks also require figures and data contained in these statements, without which a thorough analysis is impossible. All these statements may be found in the annual reports of companies.

Common methods of financial statement analysis include fundamental analysis, DuPont analysis, and the use of financial ratios. Historical information combined with a series of assumptions and adjustments to the financial information may be used to project future performance.

Analysis of Auditors Report and Opinion

The objective of the reporting phase of a financial audit is to present an informed opinion about a business's financial statements, including whether they conform to generally accepted accounting principles. Even though the report contains only three sections, the impact it can have on the future of a business makes being able to read and understand its contents crucial.

A financial audit report is the final step of an external financial audit. After planning the audit and gathering necessary information, an auditor then must interpret results. Although the information an auditor collects through inquiry, observation, inspection, calculations, comparisons and analysis is "fact," the report itself expresses the opinion of the auditor.

The introductory section identifies the responsibilities of the company director and the independent auditor. Regardless of how large the company or financial accounting department, the auditor holds the company director responsible for accounting policies, the preparation of financial documents, internal business controls designed to ensure the financial documents are honest and correct and the presentation of financial statements to the auditor. The auditor takes responsibility for expressing an opinion based only on the facts and for complying with ethical and legal auditing guidelines during the planning and information-gathering stages of the financial audit.

Scope of the audit -- the area it covers -- is the second and shortest section. It provides a description of what the auditor has done and includes a blanket statement -- a statement common to and for the most part identical in every audit report -- that specifically states the auditor has examined the financial statements of the business in accordance with generally accepted auditing standards and has performed appropriate tests to make a reasonable assessment of the business's financial processes, internal controls and documents.

Auditor's Opinion

The auditor's opinion is the most important section of the audit report. Here the auditor sums up findings by expressing one of three generally accepted opinions or includes a disclaimer, which means the auditor refuses to give an opinion, most often because the business either can't or won't produce the appropriate documents or information. The most favorable opinion is an unqualified opinion, meaning the company director provided all the necessary financial documents and everything was in order and met all auditing requirements. A qualified opinion means that while the majority of documents were in order, the auditor did find one or two exceptions. An adverse opinion is an opinion no business wants; this negative opinion says the business financial records are inaccurate, incomplete or not in compliance with generally accepted accounting principles.

Analysis of Management Judgement

Management Personal judgement plays a vital role in the preparation of financial records and financial statements. The management may use their judgement in choosing the method of valuation of closing inventory, in calculating the provision for bad debts and in choosing the method of charging the depreciation of fixed assets. Likewise, the application of various accounting concepts and conventions depends upon the personal judgement of the management. Therefore, different meaning and results can be obtained from the financial statements of the same company. Based on the different results, different recommendations may be provided for the growth and development of a business concern.

Problems in Financial Statement Analysis

Lack of an Underlying Theory The basic problem in financial statement analysis is that there is no theory that tells us which numbers to look at and how to interpret them. In the absence of an underlying theory financial statement analysis appears to be ad hoc, informal, and subjective. As Horrigan put it: "From a negative viewpoint, the most striking aspect of ratio analysis is the absence of an explicit theoretical structure. As a result the subject of ratio analysis is replete with untested assertions about which ratios should be used and what their proper levels should be."

Conglomerate Firms Many firms, particularly the large ones, have operations spanning a wide range of industries. Given the diversity of their product lines, it is difficult to find suitable benchmarks for evaluating their financial performance and condition. Hence, it appears that meaningful benchmarks may be available only for firms which have a well-defined industry classification.

Window Dressing Firms may resort to window dressing to project a favourable financial picture. For example, a firm may prepare its balance sheet at a point when its inventory level is very low. As a result, it may appear that the firm has a very comfortable liquidity position and a high turnover of inventories. When window dressing of this kind is suspected, the financial analyst should look at the average level of inventory over a period of time and not the level of inventory at just one point of time.

Price Level Changes Financial accounting, as it is currently practised in India and most other countries, does not take into account price level changes. As a result, balance sheet figures are distorted and profits misreported. Hence, financial statement analysis can be vitiated.

Variations in Accounting Policies Business firms have some latitude in the accounting treatment of items like depreciation, valuation of stocks, research and development expenses, foreign exchange transactions, installment sales, preliminary and pre-operative expenses, provision of reserves, and revaluation of assets. Due to diversity of accounting policies found in practice, comparative financial statement analysis may be vitiated.

Interpretation of Results Though industry averages and other yardsticks are commonly used in financial ratios, it is somewhat difficult to judge whether a certain ratio is 'good' or 'bad'. A high current ratio, for example, may indicate a strong liquidity position (something good) or excessive inventories (something bad). Likewise, a high turnover of fixed assets may mean efficient utilisation of plant and machinery or continued flogging of more or less fully depreciated, worn out, and inefficient plant and machinery.

Another problem in interpretation arises when a firm has some favourable ratios and some unfavourable ratios and this is rather common. In such a situation, it may be somewhat difficult to form an overall judgment about its financial strength or weakness. Multiple discriminate analysis, a statistical tool, may be employed to sort out the net effect of several ratios pointing in different directions.

Correlation among Ratios Notwithstanding the previous observation, financial ratios of a firm often show a high degree of correlation. Why? This is because several ratios have some common element (sales, for example, is used in various turnover ratios) and several items tend to move in harmony because of some common underlying factor. In view of ratio correlations, it is redundant and often confusing to employ a large number of ratios in financial statement analysis. Hence it is necessary to choose a small group of ratios from a large set of ratios. Such a selection requires a good understanding of the meaning and limitations of various ratios and an insight into the economics of the business.

Guidelines for Financial Statement Analysis

From the foregoing discussion, it is clear that financial statement analysis cannot be treated as a simple, structured exercise. The following point to be taken into consideration while analyse financial statements.

1. **Use ratios to get clues to ask the right questions:** By themselves ratios rarely provide answers, but they definitely help to raise the right questions.
2. **Be selective in the choice of ratios:** Compute scores of different ratios and easily drown into confusion. For most purposes a small set of ratios-three to seven-would suffice. Few ratios, aptly chosen, would capture most of the information that can derive from financial statements.
3. **Employ proper benchmarks:** It is a common practice to compare the ratios (calculated from a set of financial statements) against some benchmarks. These bench marks may be the average ratios of the industry or the ratios of the industry leaders or the historic ratios of the firm itself.
4. **Know the tricks used by accountants:** Since firms tend to manipulate the reported income, should learn about the devices employed by them.

5. **Read the footnotes: Footnotes sometimes contain valuable information.** They may reveal things that management may try to hide. The more difficult it is to read a footnote, the more information-laden it may be.

6. **Remember that financial statement analysis is an odd mixture of art and science:** Financial statement analysis cannot be regarded as a simple, structured exercise. It is a process requiring care, thought, common sense, and business judgment-a process for which there are no mechanical substitutes.

Going Beyond the Numbers

The tools of analysis discussed in this chapter are helpful in making business decisions, evaluating performance, and forecasting future developments. Comprehensive business analysis, however, calls for going beyond the conventional financial measures to consider qualitative factors relevant for evaluating the performance and prospects of a company. The American Association of Individual Investors (AAII) has summarised these factors as follows:

1. *Are the company's revenues tied to one key customer?* If so, the company's performance may decline dramatically if the customer goes elsewhere. On the other hand, if the relationship is firmly entrenched, this might actually stabilise sales.

2. *To what extent are the company's revenues tied to one key product?* Companies that rely on a single product may be more efficient and focused, but a lack of diversification increases risk. If revenues come from several different products, the overall bottom line will be less affected by a drop in the demand for any one product.

3. *To what extent does the company rely on a single supplier?* Depending on a single supplier may lead to unanticipated shortages, which investors and potential creditors should consider.

4. W*hat percentage of the company's business is generated overseas?* Companies with a large percentage of overseas business are often able to realise higher growth and larger profit margins. However, firms with large overseas operations find that the value of their operations depends in large part on the value of the local currency. Thus, fluctuations in currency markets create additional risks for firms with large overseas operations. Also, the potential stability of the region is important.

5. *Competition.* Generally, increased competition lowers prices and profit margins. In forecasting future performance, it is important to assess both the likely actions of the current competition and the likelihood of new competitors in the future.

6. *Future prospects.* Does the company invest heavily in research and development? If so, its future prospects may depend critically on the success of new products in the pipe line. For example, the market's assessment of a computer company depends on how next year's products are shaping up. Likewise, investors in pharmaceutical companies are interested in knowing whether the company has developed any potential blockbuster drugs that are doing well in the required tests.

7. *Legal and regulatory environment*. Changes in laws and regulations have important implications for many industries. For example, when forecasting the future of tobacco companies, it is crucial to factor in the effects of proposed regulations and pending or likely lawsuits. Likewise, when assessing banks, telecommunications firms, and electric utilities, analysts need to forecast both the extent to which these industries will be regulated in the years ahead, and the ability of individual firms to respond to changes in regulation.

LESSON ROUND-UP

- Forensic Auditing is a new concept that comprises three key ingredients:
    1. Forensic Audit Thinking—in other words thinking forensically
    2. Forensic Audit Procedures—both proactive and reactive
    3. Appropriate use of technology and Data analysis.
- Forensic Data Analysis can be used to Prevent, detect and control fraud along with other irregularities.
- Forensic data analysis is the process of gathering, summarizing, comparing, and aggregating existing different sets of data that organizations routinely collect in the normal course of business with the goal of detecting anomalies that are traditionally indicative of fraud or other misconduct.
- Rightly quoted by honorable Prime Minister during the inauguration of Institute's Golden Jubilee on October 4, 2017 that "Company Secretaries decides the Corporate Culture of India and he felt utmost contented of the fact that Company Secretaries ensures in all the ways that the companies in India follow the laws and regulations, do not mishandle the accounts, and are honest in their work.
- Among all, the role of company secretaries is expending in the era of forensic audit wherein they are crucially assisting in preventing, regulating and penalizing the instance of corporate frauds.
- Right from conducting forensic audit to examining the evidences, from finding the culprit behind the fraud to appearing in the court for submitted the testimony, a Company Secretary is apt in serving his professional excellence as a forensic auditor.
- To summarize, where forensic audit is a detailed engagement which requires the expertise of not only accounting and auditing procedures but also expert knowledge regarding the legal framework, and a forensic auditor is required to have an understanding of various frauds that can be carried out and of how evidence needs to be collected.
- In this context, Company Secretary is a Catalyst in Upholding Good Governance via Forensic Audit.
- Section 143 of Companies Act, 2013 talks about the power and duties of auditors and auditing standards.
- A forensic auditor is required to have special training in forensic audit techniques and in the legalities of accounting issues. A forensic audit has additional steps that need to be performed in addition to regular audit procedures.
- A fraud triangle is a tool used in forensic auditing that explains three interrelated elements that assist the commission of fraud- Pressure (motive), opportunity (ability to carry out the fraud) and rationalization (justification of dishonest intentions). Fraud risk is the vulnerability, a company/organization has towards those who are capable of overcoming the three elements in the fraud triangle. Fraud risk assessment is the identification of fraud risks that exist in the company/organization. The planning involves the formulation of techniques and procedures that align with the fraud risk and fraud risk management.
- Red flags are nothing but symptoms or indicator of situation of fraud. A red flag is a set of circumstances that are unusual in nature or vary from the normal activity. It is a signal that something is out of the ordinary and may need to be investigated further.
- The instance of Green Flags could be helpful in identifying are unusual signs or inconsistencies, but apparently harmless or perhaps even helpful.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. Discuss the Role of Company Secretaries in Forensic Audit.
2. What are different methods of Investigation in Forensic Audit?
3. What are Red Flags and Green Flags? Discuss.
4. Write a Note on Field Investigations.
5. What are the indicators / sign of Green Flags?
6. What are the indicators / sign of Red Flags?

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

Forensic Audit : Laws and Regulations

Lesson 12

KEY CONCEPTS

■ FCPA ■ OECD ■ UNCAC ■ IPC ■ PCA

Learning Objectives

To understand:

- Various penalised provisions of Companies Act, 2013 relating to fraud
- The provisions of Companies Act, 2013 relating to reporting of fraud.
- Reporting of fraud under various laws such as:
  1. SEBI Act, 1992
  2. Information Technology Act, 2000
  3. Insurance Act, 1938
  4. Prevention of Corruption (Amendment) Act, 2018
  5. Income Tax Act, 1961
- International laws such as :
  1. United Nations Convention against Corruption (UNCAC)
  2. Integrity Pact (IP)
  3. Foreign Corrupt Practices Act, 1977
  4. UK Bribery Act, 2010
- ICSI Anti-Bribery Code

Lesson Outline

- Introduction
- Indian Laws: Information Technology and Business Laws
- Companies Act, 2013
- Fraud Reporting under Companies Act, 2013
- Reporting of fraud by auditor
- Similar Provisions of Fraud Reporting applicable to Cost Auditor and Secretarial Auditor
- SEBI Act, 1992
- Information Technology Act, 2000
- Insurance Act, 1938
- The Companies (Auditor's Report) Order, 2020
- Penalty under the Prevention of Corruption Act, 1988
- Income Tax Act, 1961
- Indian Penal Code, 1860
- International Laws
- United Nations Convention Against Corruption
- OECD Guidelines for Multinational Enterprises relating to Combating Bribery
- The Integrity Pact (IP)
- Foreign Corrupt Practices Act, 1977
- The United Kingdom Bribery Act, 2010
- ICSI Anti-Bribery Code
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION

A forensic audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in the court of law. A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims.

In order to understand the legal consequences that a person attracts on being caught in a forensic audit, it is necessary to know about the various statutes that talk about the implementation of forensic audits in India.

Let us discuss the statutes dealing with corporate laws and empowering forensic auditors in performing their duties in its true letter and spirit. The detailed position of Laws and Regulations dealing with Corporate Fraud and also aids in achieving forensic audit would be discussed under the following heads:

1. **Indian Laws**
   - Information Technology and Business Laws
2. **International Laws**
   - UK Bribery Act
   - US Foreign Corrupt Practices Act
3. **ICSI Anti Bribery Code.**

1. INDIAN LAWS : INFORMATION TECHNOLOGY AND BUSINESS LAWS

Companies Act, 2013

Considering the consequence of corporate frauds on the growth of Corporates and Economy, the Companies Act, 2013 lists down frauds and prescribes penalties and punishments for violations.

Section 447 of the Companies Act, 2013 often now referred to as one of the draconian provision of the new Act deals with provision relating to punishment for fraud.

Section 447: *"Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than 6 months but which may extend to 10 years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to 3 times the amount involved in the fraud:*

Where the fraud in question involves public interest, the term of imprisonment shall not be less than 3 years".

The Companies Act, 2013 has provided punishment for fraud as provided under Section 447 in around 20 sections of the Act *e.g.* u/s 7(5), 7(6), 8(11), 34, 36, 38(1), 46(5), 56(7), 66(10), 75, 140(5), 206(4), 213, 229,

251(1), 266(1), 339(3), 448 *etc.* for directors, key managerial personnel, auditors and/or officers of company. Thus, the new Act goes beyond professional liability for fraud and extends to personal liability if a company contravenes such provisions.

The following table includes some sections that attract liability u/s 447. These are cognizable offences and a person accused of any such offence under these sections shall not be released on bail or bond, unless subject to the exceptions provided u/s 212(6) of the Act:

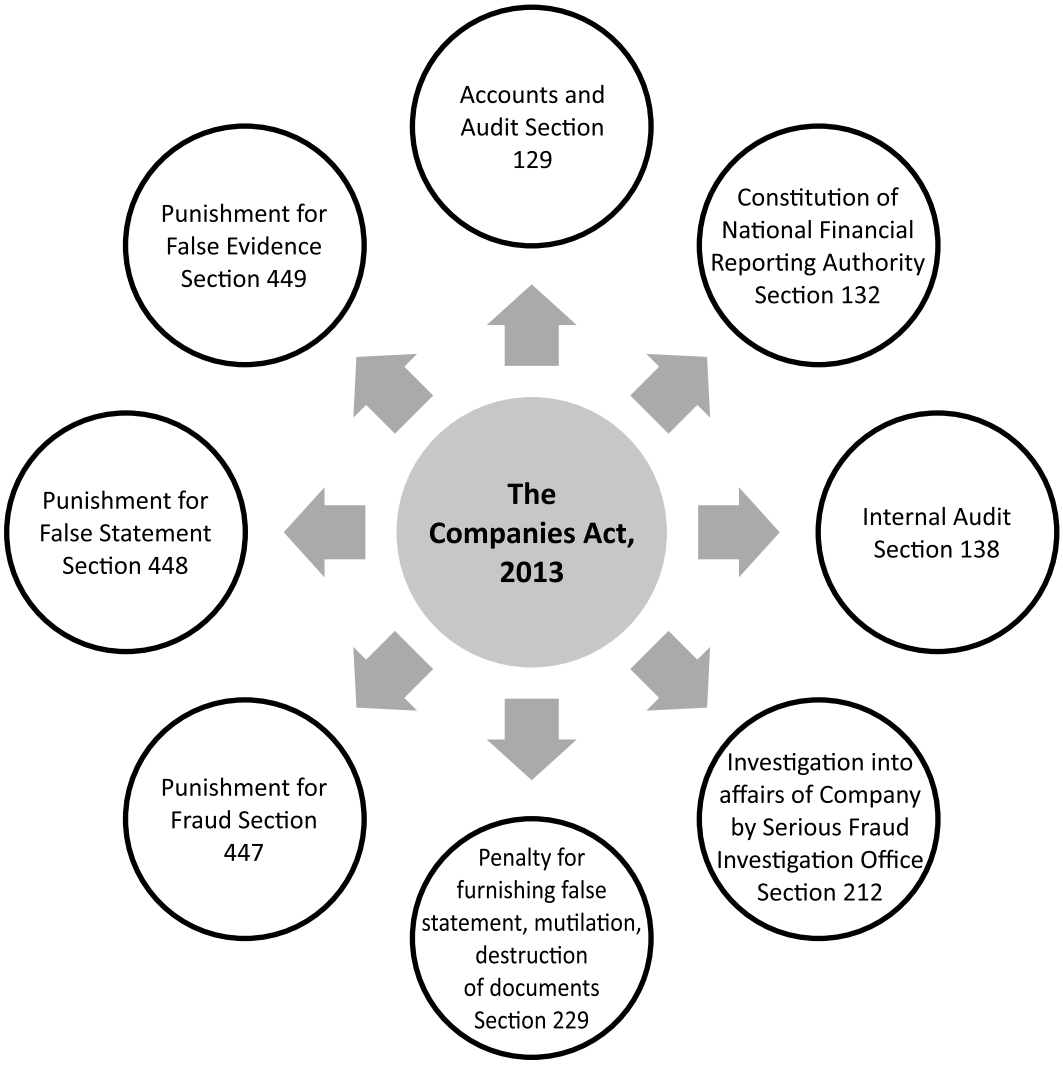
Section	***Fraud With Respect To***	***Who will be penalised***
7(5)	Registration of a company	A person furnishing false information or suppressing any material information of which he or she is aware.

Section	*Fraud With Respect To*	*Who will be penalised*
36	Inducing persons to invest money	The person doing so.
75(1)	Acceptance of deposit with intent to defraud depositors or for any fraudulent purpose	Every officer of the company who accepted the deposit.
206(4)	Conducting business of a company for a fraudulent or unlawful purpose	Every officer of the company who is in default.
213	Other cases: • Business of a company being conducted with intent to defraud its creditors • Fraud, misfeasance or other misconduct of the company or any of its members • Company withholding information from members with respect to its affairs, which they may reasonably expect	Every officer of the company who is in default and the person(s) concerned in the formation of the company or management of its affairs.
229	Furnishing false statement or mutilation or destruction of documents	Person required to provide an explanation or make a statement during the course of inspection, inquiry or investigation, or the officer or other employees, as required.
251(1)	Application for removal of name from register with the object of evading liabilities/intent to deceive	Persons in charge of management of the company.
339(3)	Conducting business of company with intent to defraud its creditors, any other persons or for any fraudulent purpose	Every person who was knowingly a party to the business in the aforesaid manner.
448	Making a false statement in any return, report, certificate, financial statement, prospectus, statement or other document required by or for the purpose of any of the provisions of this Act or the rules made thereunder.	Person making such a statement etc.

Fraud Reporting under Companies Act, 2013

The new act casts onerous responsibility on the part of statutory auditor/cost auditor/secretarial auditor to report fraud to Board and Central Government. It would mean that even for a small fraud involving say Rs. 1000 in a large multi-locational enterprise would cast reporting fraud responsibility on the part of auditing professionals including CS/CA/CMA. This provision has mandated that the professionals like CS/CA/CMA appointed by the company under Section 139/148/204 to do direct reporting of frauds (to the Central Government) in addition to their existing responsibilities of reporting requirement to the shareholder/Board of company.

Section 143(12) to 143(15) of the Act contains provisions relating to reporting of fraud.



Fraud Reporting

Section 143(12) Notwithstanding anything contained in this section, if an auditor of a company, in the course of the performance of his duties as auditor, has reason to believe that an offence involving fraud is being or has been committed against the company by officers or employees of the company, he shall immediately report the matter to the Central Government within such time and in such manner as may be prescribed.

Action of Fraud Reporting in good faith

Section 143 (13) No duty to which an auditor of a company may be subject to shall be regarded as having been contravened by reason of his reporting the matter referred to in sub-section (12) if it is done in good faith.

Similar Provisions applicable to Cost Auditor and Secretarial Auditor:

Section 143(14) the provisions of this section shall *mutatis mutandis* apply to –

- The Cost Accountant in practice conducting cost audit under section 148; or
- The Company Secretary in practice conducting secretarial audit under section 204.

Punishment for default

Section 143 (15) If any auditor, cost accountant or company secretary in practice do not comply with the provisions of sub-section (12), he shall be punishable with fine which shall not be less than 1 lakh rupees but which may extend to 25 lakh rupees.

Rule 13 of The Companies (Audit and Auditors) Rules, 2014 contains the operational procedure of Reporting of Fraud prescribed in Section 143(12) of the Act.

Reporting of fraud by Auditor

Rule 13(1) For the purpose of sub-section 12 of Section 143, in case the auditor has sufficient reason to believe that an offence involving fraud, is being or has been committed against the company by officers or employees of the company, he shall report the matter to the Central Government immediately but not later than 60 days of his knowledge and after following the procedure indicated herein below:

First Fraud Report to Board/Audit Committee

a. Auditor shall forward his report to the Board or the Audit Committee, as the case may be, immediately after he comes to knowledge of the fraud, seeking their reply or observations within 45 days;

Final Fraud Report to Central Government on receipt of First Fraud Report

b. on receipt of such reply or observations the auditor shall forward his report and the reply or observations of the Board or the Audit Committee along with his comments (on such reply or observations of the Board or the Audit Committee) to the Central Government within 15 days of receipt of such reply or observations;

Final Fraud Report to Central Government on failure of receipt of First Fraud Report

c. in case the auditor fails to get any reply or observations from the Board or the Audit Committee within the stipulated period of 45 days, he shall forward his report to the Central Government along with a note containing the details of his report that was earlier forwarded to the Board or the Audit Committee for which he failed to receive any reply or observations within the stipulated time.

Authority and Mode/Format of dispatching Final Fraud Report to Central Government

- Rule 13(2): The report shall be sent to the Secretary, Ministry of Corporate Affairs in a sealed cover by Registered Post with Acknowledgement Due or by Speed post followed by an e-mail in confirmation of the same.
- Rule 13(3): The report shall be on the letter-head of the auditor containing postal address, e-mail address and contact number and be signed by the auditor with his seal and shall indicate his Membership Number.
- Rule 13(4): The report shall be in the form of a statement as specified in Form ADT-4. This Form of Report is available as an annexure to The Companies (Audit and Auditors) Rules, 2014.

Similar Provisions of Fraud Reporting applicable to Cost Auditor and Secretarial Auditor

Rule 13(5): The provision of this rule shall also apply, mutatis mutandis, to a cost auditor and a secretarial auditor during the performance of his duties under Section 148 and section 204 respectively.

The new law has also bestowed legal status on the Serious Fraud Investigation Office, a probe agency under the Ministry of Corporate Affairs. Serious Fraud Investigation Office (SFIO) is established by Central Government to investigate frauds relating to a company.

SEBI Act, 1992

Regulation 11 C of the SEBI Act, 1992 empowers the SEBI to direct any person to investigate the affairs of intermediaries or brokers associated with the securities market whose transactions in securities are being dealt with in a manner detrimental to the investors or the securities market.

Information and Technology Act, 2000

Section 43 and 44 of the IT Act, 2000- lays down penalty for the following

- Unauthorized copying of an extract from any data.
- Unauthorized access and downloading files.
- Introduction of viruses or malicious programmes.
- Damage to a computer system or computer network.
- Denial of access to an authorized person to a computer system.
- Providing assistance to any person to facilitate unauthorized access to a computer.

Insurance Act, 1938

Section 33 of the Act empowers the IRDA to direct any person (Investigating Authority) to investigate the affairs of any insurer.

The Companies (Auditor's Report) Order, 2020

The Act requires the auditor to report to the effect that if a substantial part of fixed assets have been disposed of during the year, whether it has affected the going concern status. In light of these statutory authorities, the following penalties may be faced by a person, if he/she is caught in a forensic audit, by way of white-collar penalties.

Penalty under the Prevention of Corruption Act, 1988 (PC Act)

Prevention of Money-Laundering Act, 2002– Section 3 of the Act defines the offence of money laundering as the involvement of a person in any process or activity connected with the proceeds of crime and projecting it as untainted property, where the scope of integrating forensic audits can be clearly seen.

The Prevention of Corruption (Amendment) Act, 2018: An Abridged

The Prevention of Corruption Act, 1988 (the "Act") was amended by the Prevention of Corruption (Amendment) Act, 2018 (the "Amendment Act"). Most of the amendments are aimed at tightening up the existing provisions in the Act and expanding the coverage of the offences. Prevention of Corruption (Amendment) Act 2018 as passed by Parliament in July 2018, which amended and brought about significant changes to the extant Prevention of Corruption Act 1988. Among other changes, the Amendment Act has made bribe giving a specific offence and has introduced the concept of corporate criminal liability for acts of bribery. Corporates may claim a defence if it can be proven that adequate procedures were in place to prevent persons associated with it from undertaking anything which may be an offence under the Prevention of Corruption Act. Such procedures must comply with guidelines, which are yet to be prescribed by the government.

Backdrop of the Amendment Act

In the wake of numerous scams being unearthed in India over the past decade, enforcement agencies have also been proactive in terms of monitoring compliance under relevant anti-corruption and bribery laws and taking action against violations.

In 2016 the government announced demonetisation of Rs 500 and Rs 1000 bank notes in its attempt to combat unethical practices such as hoarding black money outside the formal economic system, tax evasion and using illicit or counterfeit cash to fund illegal activities. Consequently, on basis of information received from banks, the tax authorities and other anti-corruption bodies have identified suspicious persons and entities and initiated action against them.
In 2017 the Ministry of Corporate Affairs voluntarily struck off 224,000 shell companies and imposed restrictions on the usage of their bank accounts and transference of company property.
Action was taken to disqualify directors who failed to comply with specific requirements under the Companies Act 2013.
The ministry also announced that if any director or other authorized signatory of a struck-off company tried to siphon off money from the company's bank account, he or she will be punished with a prison term of between six months and 10 years, and where the fraud involved public interest, the minimum prison term will be at least three years and may also involve a fine of up to three times the amount involved.
The prime minister's office has created a special task force to oversee the drive against such defaulting companies with the help of various enforcement agencies.
Further, in 2018 an ordinance to the Companies Act 2013 was promulgated reintroducing the requirement to declare the commencement of business for newly incorporated companies, which may restrict the opening of shell companies.
The Central Vigilance Commission (CVC) has also taken certain proactive actions recently, such as advising all central government departments on quicker disposal of pending corruption cases. The CVC has an online complaint management system where individuals can register complaints in this regard.
The Serious Fraud Investigation Office (the investigative arm of the Ministry of Corporate Affairs) has increased the pace of its investigations over the past couple of years. Moreover, the Supreme Court has expanded the ambit of the definition of 'public servant' (under the Prevention of Corruption Act 1988) to include all officials of private banks, as their duties are public in nature (Central Bureau of Investigation, Bank Securities and Fraud Cell v. Ramesh Gelli, February23, 2016) thereby bringing them under the purview of anti-corruption laws.

Highlights of the Prevention of Corruption (Amendment) Act, 2018

Definition of 'Undue Advantage': The Amendment Act provides that any public servant who accepts or attempts to accept from any person, any 'undue advantage', either for himself or for any other person, in lieu of performance of a public duty, shall be punishable with imprisonment for a minimum term of 3 (three) years and maximum of 7 (seven) years. The Amendment Act has defined 'undue advantage' to mean any gratification other than legal remuneration that a public servant is permitted to receive. Further, 'gratification' is not limited to pecuniary gratifications or to gratifications estimable in money. By virtue of such an expansive definition, even non-monetary considerations such as a better posting, post-retirement benefits, gifts and favours not estimable in money can also be covered under the ambit of undue advantage.

Persons liable for offering a bribe to public servants: Previously, the PC Act did not contain a separate provision for a person who gives or promises to give an undue advantage, but the Amendment Act makes giving an undue advantage by a person to a public servant, a specific offence punishable by 7 (seven) years imprisonment or fine, or both. However, if a person is forced / coerced to give an undue advantage but reports the same to the

concerned authority within 7 (seven) days of doing so, he shall not be liable for the same. Further, as per the PC Act, during a corruption trial, if a person made a statement that he gave an undue advantage to a public servant, it would not be used to prosecute him for the offence of abetment. The Amendment Act omits this provision. Effectively, it may become a potential risk for bribe givers to testify against the corrupt, and they may be discouraged from appearing as witnesses in a trial against public servants.

Offering of bribes by commercial organisations: The Amendment Act has defined 'commercial organisation' to mean not just a company or partnership incorporated in India and carrying on business in India or outside India, but also a body or partnership incorporated or formed outside India but carrying on business in India. Section 9 of the PC Act has been substituted by the Amendment Act to provide for a specific provision for offences committed by commercial organisations and persons associated with it. It provides that if a commercial organisation commits any of the offences listed out in the PC Act with the intention to obtain or retain business or obtain or retain an advantage in the conduct of its business, then such commercial organisation shall be punishable with fine, quantum of which is not prescribed in the Amendment Act.

The Amendment Act mandates the Central Government to formulate and prescribe guidelines to prevent persons associated with commercial organisations from bribing any public servant. A commercial organisation can defend itself when accused of any offence under the PC Act, if it proves that it had adequate procedures in place to ensure compliance with such guidelines issued by the Central Government to prevent persons associated with the commercial organisation from undertaking such conduct. The corporate sector in India will have to be swift in enacting its internal guidelines and ensure that its employees are well informed and abide by these guidelines to protect itself from any kind of prosecution under the PC Act, in the event of any associated person charged with the act of giving a bribe.

Further, if such an offence is proved to have been committed with the consent or connivance of any director, manager, secretary or other officer of the organisation, then such person shall also be prosecuted under the PC Act.

Redefining criminal misconduct: Under the PC Act, criminal misconduct by a public servant inter alia included: (i) using illegal means to obtain any valuable thing or monetary reward for himself or any other person; (ii) abusing his position as a public servant to obtain a valuable thing or monetary reward for himself or any other person; and (iii) obtaining a valuable thing or monetary reward without public interest, for any person. The Amendment Act replaces this section with a truncated definition of criminal misconduct to include only the following two acts: (i) misappropriation or conversion for his own use, any property entrusted to or under the control of a public servant: and (ii) amassing assets disproportionate to known sources of income. To prove the latter, the intention to acquire assets disproportionate to income must also be proved, in addition to possession of such assets. Thus, the scope of criminal misconduct has been narrowed and the threshold to establish the offence of possession of disproportionate assets has been increased by the Amendment Act.

Prior sanction of appropriate government for investigation and prosecution: The PC Act required prior sanction of the appropriate government for prosecution of serving public officials. The Amendment Act extends this protection of requirement of prior approval to investigation prior to prosecution. Further, such protection is extended to former officials as well, for offences done while in office. The third proviso to Section 19(1) provides for a directory (not mandatory) time period of 3 (three) months within which the appropriate government must convey the decision on such sanction. Additionally, the Central Government may prescribe guidelines for grant of sanction for prosecution.

Attachment of property: The Amendment Act has provided for application of the Prevention of Money Laundering Act 2002 and Criminal Law Amendment Ordinance 1944 for attachment and administration of property procured by means of an offence under the PC Act.

Time frame for trial: The PC Act did not provide a time frame within which the trial was to be completed. However, the Amendment Act now prescribes that the Special Judge shall endeavour to complete the trial within 2 (two) years. This period can be extended by 6 (six) months at a time and up to a maximum of 4 (four) years in aggregate subject to proper reasons for the same being recorded. The wording of the section is directory in nature and not mandatory, making it less likely that the courts will abide by such timelines.

Enhancement of Punishment: Punishment has been increased from a minimum imprisonment term of 6 (six) months to 3 (three) years, and from a maximum of 5 (five) years to 7 (seven) years, with or without fine. Punishment for abetment of offences has also been increased by the same quantum.

Income Tax Act, 1961

Though Income Tax Act does not deal with corruption directly but contains number of provisions which deal with ill-gotten money by an assesse.

Cash Credits [Section 68]: As per the provision of Section 68 of the Act, any sum found credited in the books of an assessee maintained for any previous year, and the assessee offers no explanation about the nature and source thereof or the explanation offered by him is not, in the opinion of the Assessing Officer, satisfactory, the sum so credited may be charged to income-tax as the income of the assessee of that previous year.

Unexplained Investments [Section 69] : As per the provision of Section 69 of the Act, where in the financial year immediately preceding the assessment year the assessee has made investments which are not recorded in the books of account, if any, maintained by him for any source of income, and the assessee offers no explanation about the nature and source of the investments, or the explanation offered by him is not, in the opinion of the Assessing Officer, satisfactory, the value of the investments may be deemed to be the income of the assessee of such financial year.

Unexplained Money [Section 69A] : As per the provision of Section 69A of the Act, where in any financial year the assessee is found to be the owner of any money, bullion, jewellery or other valuable article and such money, bullion, jewellery or the valuable article is not recorded in the books of account, if any, maintained by him for any source of income, and the assessee offers no explanation about the nature and source of acquisition of the money, bullion, jewellery or other valuable article, or the explanation offered by him is not, in the opinion of the Assessing Officer, satisfactory, the money and the value of the bullion, jewellery or other valuable article may be deemed to be the income of the assessee for such financial year.

Amount of investments, etc., not fully disclosed in books of account [Section 69B]: As per the provision of Section 69B of the Act, where in any financial year the assessee has made investments or is found to be the owner of any bullion, jewellery or other valuable article, and the Assessing Officer finds that the amount expended on making such investments or in acquiring such bullion, jewellery or other valuable article exceeds the amount recorded in this behalf in the books of account maintained by the assessee for any source of income, and the assessee offers no explanation about such excess amount, or the explanation offered by him is not, in the opinion of the Assessing Officer, satisfactory, the excess amount may be deemed to be the income of the assessee for such financial year.

Unexplained Expenditure [Section 69C]: As per the provision of Section 69C of the Act, where in any financial year an assessee has incurred any expenditure and offers no explanation about the source of such expenditure or part thereof, or the explanation, if any, offered by him is not, in the opinion of the Assessing Officer, satisfactory, the amount covered by such expenditure or part thereof, as the case may be, may be deemed to be the income of the assessee for such financial year.

Tax on income referred to in Section 68 or Section 69 or Section 69A or section 69B or Section 69C or section 69D is chargeable to tax under Section 115BBE which provides that on any such income the income-tax payable shall be the amount of income-tax calculated at the rate of 60%.

As per the provision of Section 271AAC of the Act, where the income determined includes any income referred to in Section 68, Section 69, Section 69A, Section 69B, Section 69C or Section 69D for any previous year, the assessee shall pay by way of penalty, in addition to tax payable under Section 115BBE, a sum computed at the rate of 10% of the tax payable under Section 115BBE.

Indian Penal Code, 1860

- Section 168 of the IPC – Public servant unlawfully engaging in trade: "Whoever, being a public servant, and being legally bound as such public servant not to engage in trade, engages in trade, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both."
- Section 171 B – Bribery, read with Section 7 of the PC Act "Whoever commits the offence of bribery shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both. Provided that bribery by treating shall be punished with fine only" as per Section 171E.
- Section 403 – Dishonest Misappropriation of property.
- Section 405 – Criminal Breach of Trust: "Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both" according to Section 406.
- Section 417 – Cheating.
- Section 463 – Forgery "Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine or with both" Penalties under Prevention of Money Laundering Act, 2002.
- Section 4 – Punishment for money-laundering. –

Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees:

Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted.

2. INTERNATIONAL LAWS

Corruption is a political, social and economic issue at the global level. The issue of corruption cuts to the heart of modern ideas about politics, culture and democracy. Despite continuing concern and a multi-million dollar international industry committed to fighting it, corrupt practices often seem impervious to change. Today it is a major cause of global crises of poverty, human rights violation, injustice and insecurity.

Many governments have been launched anticorruption policies and programmes in order to combat corruption. Although, over a period of time, the number of proposals and ideas on different ways and means to combat corruption has grown, the progress is less than satisfactory.

A less corrupt country likely to have more growth, improved foreign investments, higher per capita income, lower infant mortality, increased literacy, stronger property rights, increased business growth and many other additional benefits. The challenges are how to get from here to there. In this direction, let us take a brief look on the International Laws, Regulations and Treating holding strong in preventing corruption from their system.

United Nations Convention against Corruption (UNCAC)

The United Nations Convention against Corruption "UNCAC" is a multilateral treaty or agreement that has been negotiated by member states of the United Nations, "UN", and promoted by the UN Office on Drugs and Crime, "UNODC". It is one of the several legally binding international anti-corruption agreements that require state parties to abide by the treaty to implement several anti-corruption measures and mainly focus on five main areas as follows:

The UNCAC's comprehensive approach and the mandatory character of many of its provisions act as evidences of this development. Most importantly, the UNCAC tackles the forms of corruption that had not been covered by many of the earlier international instruments, such as trading under influence, abuse of function, and various other types of corruption in the private sector. A further important significant development is the specific inclusion of a provision dealing with the recovery of stolen assets, which is a major concern for countries.[6]

OECD Guidelines for Multinational Enterprises relating to Combating Bribery

The Guidelines for Multi-National Enterprises (MNEs) prescribed by the OECD are the most wide-ranging set of government-supported recommendations on responsible business conduct in existence today. The Governments adhering to the guidelines aim to encourage and maximize the positive impact of the MNEs for sustainable development and enduring social progress. It provides guidance for responsible business conduct in areas, such as, labour rights, human rights, environment, information disclosure, combating bribery, consumer interests, competition, taxation, and intellectual property rights.

The Integrity Pact (IP)

The Integrity Pact is a tool developed and launched by the Transparency International to help different businesses, governments and civil societies in order to equip them to fight corruption in the field of public procurements and public contracting. The Transparency International had established mutual contractual rights and obligations to reduce the high cost and corruption involved in the public contracts. The main objective of the Integrity pact is to make the public procurement process transparent by binding both the parties to the contract. It also envisages a monitoring role for civil society who is the ultimate beneficiary of government action. IP should cover all activities related to the contract from pre-selection of bidders, bidding and contracting, implementation, completion and operation.

Foreign Corrupt Practices Act, 1977 (U.S.A.)

The Foreign Corrupt Practices Act, 1977 "FCPA" is a United States' federal law that contains two main provisions, *i.e.*, addresses accounting transparency requirements under the Securities Exchange Act of 1934 and concerning bribery of foreign officials. The Act was amended in 1988 and further in 1998. It includes both bribery and accounting provisions.

Applicability of the Act

- Any person who has a certain degree of connection with the United States and engages in foreign corrupt practices.
- Any act by U.S. businesses, foreign corporations trading securities in the U.S., American nationals, citizens, and residents acting in furtherance of a foreign corrupt practice whether or not they are physically present in the U.S.
- In the case of foreign natural and legal persons, the Act covers their deeds if they are in the U.S. at the time of the corrupt conduct.

The ideology of the FCPA is to make it illegal for companies and their supervisors to influence foreign officials with any personal payments or rewards. This Act was passed to make it unlawful for certain classes of people and entities to make payments to foreign government officials in order to assist in obtaining or retaining business. Further, the Act governs not only payments to foreign officials, candidates, and parties, but any other recipient if part of the bribe is ultimately attributable to a foreign official, candidate, or party. These payments are not restricted to monetary forms and may include anything of value. This is considered the territoriality principle of the Act.

Under the FCPA it must be proved that the person offering the bribe did so with a "corrupt" intent. Further, the FCPA only covers active bribery, that is to say the giving of a bribe. The taking of the bribe is not covered under the FCPA. The Act concerns the intent of the bribery rather than the amount, and therefore there is no requirement of materiality. Offering anything of value as a bribe, whether in the form of cash or non-cash items, is prohibited.

***Accounting Provision**:* The FCPA also requires the companies whose securities are listed in the U.S. to meet its accounting provisions. These accounting provisions operate in tandem with the anti-bribery provisions of the FCPA, and requires respective corporations to prepare and keep books and records that accurately and fairly reflect the transactions of the corporation, and to devise and maintain an adequate system of internal accounting controls. An increasing number of corporations are taking additional steps to protect their reputation and reduce their exposure by employing the services of due diligence companies tasked with vetting third party intermediaries and identifying easily overlooked government officials embedded in otherwise privately held foreign firms.

***Bribery and facilitation payment**:* With reference to payments to foreign officials, the act draws a distinction between bribery and facilitation or "grease payments", which may be permissible under the FCPA, but may still violate local laws. The primary distinction is that grease payments or facilitation payments are made to officials to expedite their performance of the routine duties which they are already bound to perform. The exception focuses on the purpose of the payment rather than on its value.

***Successor's liability for the FCPA violation**:* The Act provides that U.S. Company acquiring a foreign firm could face successor liability for the FCPA violations committed by the foreign firm prior to being acquired. Generally, acquiring companies may be liable as a successor for pre-existing the FCPA violations committed by an acquired company where those violations were subject to the FCPA's jurisdiction when committed.

Further, businesses increasingly focus on their core competencies, and as a result engage more third parties

to provide critical business functions; businesses do not have direct control over their third parties and as such, are exposed to the regulatory and reputational risk of the third party FCPA violations. As per the FCPA, businesses bear accountability for activities involving both their internal and external relationships. Companies who operate internationally, or who engage third parties in countries with a high Corruption Perceptions Index are especially at risk. Many companies have now adopted "Anti-Bribery/Anti-Corruption" (ABAC) solutions to combat this risk and help protect themselves from fines and reputational damage.

Penalty

For offences committed under the FCPA an individual can be fined up to US $ 250,000 per violation, and may also be given upto five years of imprisonment. A company guilty under the FCPA is liable for a fine of up to US $ 2,000,000 per violation.

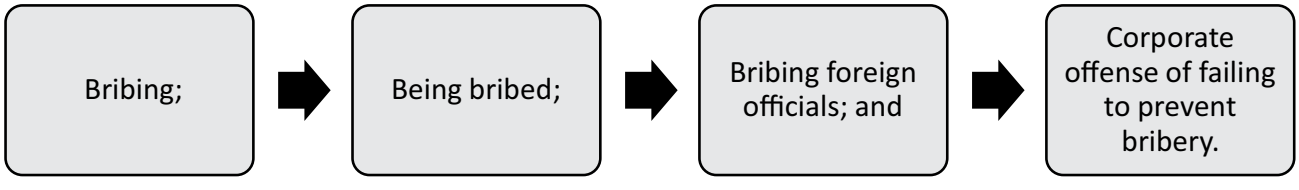
The United Kingdom Bribery Act, 2010

The Bribery Act, 2010 is an Act of the Parliament of the United Kingdom that covers the criminal law relating to bribery. The Act defines all the previous statutory and common law provisions in relation to bribery, the bribery of foreign public officials and the failure of a commercial organisation to prevent bribery on its behalf.

The objective of the Act is to provide a modern legislation that effectively deals with the increasingly sophisticated, cross-border use of bribery, and carry out the prosecution of bribery by individuals and organizations both within the UK and overseas easier. It applies to the United Kingdom of Great Britain and Northern Ireland.

Salient features of the Act

- It will criminalise both active and passive bribery, i.e., both bribing and being bribed.
- It will criminalise not just bribery of public officials, but also bribery entirely in the private sphere.
- It does not require proof of dishonesty or corruption.
- It will criminalise the failure to prevent bribery.
- It will, effectively, require those carrying on business in the UK to have in place "adequate procedures" to prevent bribery taking place, even if the bribery is unconnected with the UK.
- The offences will have extensive extra-territorial reach, criminalising activities which may take place entirely outside the UK.
- Committing offences could lead to imprisonment for up to 10 years (for individuals) and/or unlimited fines (for individuals and corporate bodies).
- There is no exception for "facilitation payments".
- "Local customs and practices" will not necessarily provide a defence.
- The Act creates four offences of bribery such as:



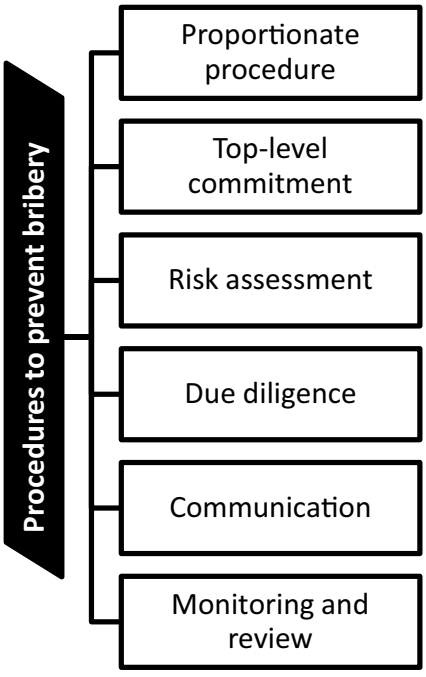
Bribing: Section 1 of the Act provides that it is an offence for a person to offer, promise or give a financial or other advantage for the purpose of bringing about an improper performance of a function or activity.

Being bribed: Section 2 of the Act provides that it is an offence to request, agree to or receive a financial or other advantage for the purpose of bringing about an improper performance of a function or activity or to request, agree to or receive a reward for having done so.

Bribery of Foreign Public Official: Section 6 of the Act provides that it is an offence to offer, promise or give a financial or other advantage to a foreign public official where such advantage is not permitted under the written law applicable to that foreign official. Further, the bribery giver must intend that the advantage given or offered would influence the foreign official in the performance of his/her duties as a public official and must intend to secure business, or to obtain a business advantage. However, the defence is available if the local laws of the country of the foreign official permit or require them to be influenced in that way.

Corporate offence of failing to prevent bribery: Section 7 of the Act provides that a commercial organisation commits an offence under the Act if a person associated with it bribes another person with an intention of obtaining or retaining either business or a business advantage for that organization. However, the commercial organisations will have an absolute defence to liability if they can show that they have put in place "adequate procedures" to prevent bribery. The personal liability can be put in place on senior company officers who turn a blind eye to such board-level bribery.

Adequate procedures to prevent bribery: The UK Bribery Act also specifies what could be considered as adequate procedure put in place to prevent bribery. This will include:



- *Proportionate procedures* – the procedures adopted should be proportionate to the risk faced.
- *Top-level commitment* – the company should adopt a culture of zero tolerance through a commitment by senior management.
- *Risk assessment* – the company should identify its bribery risks and priorities its actions in high risk areas.
- *Due diligence* – the company should take appropriate care when entering into relationships or markets where there is a risk of bribery.

- *Communication* – the company's policy should be clearly communicated to all relevant parties, supported by appropriate training and "speak up" procedures.
- *Monitoring and review* – the procedures put in place should be reviewed and updated as the company's risks change over time.

Penalties

An individual found to have committed an offence under the Bribery Act is liable to be awarded imprisonment for up to ten years and/or to an unlimited fine. A company found guilty is subject to an unlimited fine.

3. ICSI ANTI BRIBERY CODE

Indeed, we have plethora of legislations to fight against the menace of corruption and bribery, yet, if we hold a comparative analysis of legal measures India hold in effectively combating corruptions and bribery with the international practices of the related area, we find that though India has various anti-corruption legislations and anti-corruption institutions, yet the main legislation 'Prevention of Corruption Act, 1988' does not contain any provision directly dealing with the offence of giving bribe. In the Companies Act, 2013, also the offence of corruption or bribery is not specified. It is only a matter of time that India will have a specific legislation (Act) to deal with bribery in the private sector. In international legislations like the Foreign Corrupt Practices Act, 1977.

(FCPA) of USA and the United Kingdom Bribery Act, 2010 both, mandate corporate and other business entities to formulate and adopt anti-bribery policies in accordance with its requirements and provide protection to senior management if they have Anti-Bribery policy in place.

In a survey of the corporate sector by the ICSI, it was observed that due to absence of clear-cut guidelines, the private sector lacks a well-formulated policy to check corruption and the supply side of bribery emanating in their organisations.

Continuing with our deep-rooted perseverance in going hand in hand with the government's initiative towards the practices of good governance and inclusive growth of nation, the Institute is dedicating all its efforts in making India to quit corruption and bribery in its entirety. As a step forward in this dedication towards corruption free India, the Institute is recommending 'Corporate Anti-Bribery Code' (The Code) to apprise the stakeholders about the deep effect, impact of corruption on the growth of corporates and the laws to check and regulate the practices of bribery and corruption in the corporates.

Need for the Code

The main legislation 'Prevention of Corruption Act, 1988' dealing with corruption at present does not provide a definition of 'Corruption' itself. Also, in any corrupt transaction, there are two parties: the bribe-giver and the bribe- taker, but as per Section 24 of the Act, a statement made by a bribe-giver in any proceeding against a public servant for an offence, shall not subject him to prosecution under Section 12. This Act, also does not contain any provision directly dealing with active domestic bribery, *i.e.*, the offence of giving bribe. The Code seeks to curb the supply side of corruption prevalent in the private sector and also covers surrogate corrupt practices.

Objective

The objective of the Code is to ensure that neither the company nor any of its employees, directors or authorised representatives indulge in bribery in any of their actions taken for and on behalf of the company in the course of economic, financial or commercial activities of any kind.

Scope

'Corporate Anti-Bribery Code' (The Code), may be adopted voluntarily by the Corporates. The Code, once adopted by the Company, shall be applicable to the company and its:

- Board of Directors,
- Employees (full time or part-time or employed through any third party contract),
- Agents, Associates, Consultants, Advisors, Representatives and Intermediaries, and
- Contractors, Sub-contractors and Suppliers of goods and/or services.

ICSI Anti-Bribery Code: A Way Ahead

In the present scenario, when with a view to eradicate corruption from its core, people of the nation are called upon to leave the attitude of *"Chalta hai"* and to adopt the attitude of *"Badal Sakta hai"* for the inclusive growth of nation, a step forward would surely be a great association in the governments' fight against black money and corruption while establishing transparent governance at an upper end. It is beautifully said that everyone with their core strength hold the sky, then a sky of malicious act would never fall on the good of the people. In this line this Code would be a step forward in acquainting the stakeholders about the deep effect and impact of corruption on the growth of corporates along with the laws to check and regulate the practices of bribery and corruption in the corporates. This would surely advance their proficiencies in assisting the government's initiative towards building a corruption free New India.

"There is no compromise, when it comes to corruption, you have to fight it"

LESSON ROUND-UP

- The detailed position of Laws and Regulations dealing with Corporate Fraud and also aids in achieving forensic audit would be discussed under the following heads:
    1. Indian Laws
    2. Information Technology and Business Laws
    3. International Laws
    4. UK Bribery Act
    5. US Foreign Corrupt Practices Act
    6. ICSI Anti Bribery Code.
- Considering the consequence of corporate frauds on the growth of Corporates and Economy, the Companies Act, 2013 lists down frauds and prescribes penalties and punishments for violations.
- Section 447 of the Companies Act, 2013 often now referred to as one of the draconian provision of the new Act deals with provision relating to punishment for fraud.
- The Companies Act, 2013 has provided punishment for fraud as provided under Section 447 in around 20 sections of the Act e.g. u/s 7(5), 7(6), 8(11), 34, 36, 38(1), 46(5), 56(7), 66(10), 75, 140(5), 206(4), 213, 229, 251(1), 266(1), 339(3), 448 etc. for directors, key managerial personnel, auditors and/or officers of company.
- The new act casts onerous responsibility on the part of statutory auditor/cost auditor/secretarial auditor to report fraud to Board and Central Government.

- Section 143 (15) If any auditor, cost accountant or company secretary in practice do not comply with the provisions of sub-section (12), he shall be punishable with fine which shall not be less than 1 lakh rupees but which may extend to 25 lakh rupees.
- Rule 13 of The Companies (Audit and Auditors) Rules, 2014 contains the operational procedure of Reporting of Fraud prescribed in Section 143(12) of the Act.
- Rule 13(5): The provision of this rule shall also apply, mutatis mutandis, to a cost auditor and a secretarial auditor during the performance of his duties under Section 148 and section 204 respectively.
- Regulation 11 C of the SEBI Act, 1992 empowers the SEBI to direct any person to investigate the affairs of intermediaries or brokers associated with the securities market whose transactions in securities are being dealt with in a manner detrimental to the investors or the securities market.
- Section 33 of the Act empowers the IRDA to direct any person (Investigating Authority) to investigate the affairs of any insurer.
- Section 3 of the Act defines the offence of money laundering as the involvement of a person in any process or activity connected with the proceeds of crime and projecting it as untainted property, where the scope of integrating forensic audits can be clearly seen.
- Major International Laws covering this domain are:
    1. United Nations Convention Against Corruption (UNCAC)
    2. OECD Guidelines for Multinational Enterprises relating to Combating Bribery
    3. The Integrity Pact (IP)
    4. Foreign Corrupt Practices Act, 1977
    5. The United Kingdom Bribery Act, 2010
- Continuing with our deep-rooted perseverance in going hand in hand with the government's initiative towards the practices of good governance and inclusive growth of nation, the Institute is dedicating all its efforts in making India to quit corruption and bribery in its entirety.
- As a step forward in this dedication towards corruption free India, the Institute is recommending 'Corporate Anti-Bribery Code' (The Code) to apprise the stakeholders about the deep effect, impact of corruption on the growth of corporates and the laws to check and regulate the practices of bribery and corruption in the corporates.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. Discuss the Civil Remedies available against Fraud in India
2. Write a brief note on ICSI Anti – Bribery Code.
3. What are provisions in Information Technology to prevent and regulate Corporate Frauds in India?

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

Forensic Audit and Indian Evidence Law

Lesson 13

KEY CONCEPTS

■ Evidence ■ Primary Evidence ■ Secondary Evidence ■ Opinion Evidence ■ Facts ■ Question of Fact ■ Question of Law ■ Relevant Facts ■ Adducing evidence

Learning Objectives

To understand:

- The classification of Evidence, i.e., Primary and Secondary
- What is Facts and its examples?
- What is Evidence under Indian Evidence Act?
- Understand about finding facts as per Indian Evidence Act
- What is Question of Fact and Question of Law?
- The various types of Evidences.
- Understand the meaning of relevant Facts as per the Act along with examples
- Understand about admission of evidence
- What are the various methods to prove cases?

Lesson Outline

- Background to Forensic Audit and the Indian Evidence Act, 1872
- Finding Facts
- Question of Facts
- Question of Law
- Types of Evidences
- Meaning of Relevant Fact
- Admission of Evidence
- Method to Prove Cases
- Proving a matter through evidences on the basis of sources
- Procedure to be performed while doing Forensic Audit
- Case Study
- Lesson Round-Up
- Test Yourself
- List of Further Readings

BACKGROUND TO FORENSIC AUDIT AND THE INDIAN EVIDENCE ACT, 1872

We learnt in previous lessons that forensic audit is a specialised type of audit that involves the application of accounting, investigative, and legal skills to examine and evaluate financial information for use in legal proceedings. In India and across the world, forensic audits are becoming increasingly important in cases of financial fraud, corruption, bribery, embezzlement, Bankruptcy fraud and other white-collar crimes.

Forensic audit is the application of forensic techniques in financial analysis to investigate and establish evidence in a legal dispute or investigation. The forensic audit is done to gather evidence that can be used in a court of law to prove or disprove a legal claim.

The Indian Evidence Act ('the Act") is a legislation that governs the admissibility and use of evidence in Indian courts of law. It was enacted in 1872 and has been amended several times since then to keep up with changing times and legal requirements. It came into force on the first day of September, 1872. The Act applies to all judicial proceedings in India, both civil and criminal.

The Act plays an important role in determining the admissibility and weight of evidence in cases involving forensic audits. By understanding the rules and principles of evidence law, forensic auditors can ensure that their findings are presented in a manner that is admissible and persuasive in court.

The Act provides the framework for the admissibility and relevance of evidence in legal proceedings. Under the Act, evidence can be classified as oral, documentary, or material, and must be relevant and admissible to be considered in a court of law.

The Act defines different types of evidence, such as direct evidence, circumstantial evidence, and hearsay evidence. It also sets forth the rules for presenting evidence, such as the requirement that evidence must be relevant and admissible.

The Act governs the admissibility, relevance of evidence and proof of documentary evidence, including the rules for proving handwriting, electronic records, and public documents in legal proceedings. The Act also covers the admissibility of expert evidence, documentary evidence, and electronic evidence. It sets out the requirements for the admissibility of each type of evidence and how it should be presented in court.

Under the Act, evidence can be classified into two types: Primary evidence and Secondary evidence.

Primary Evidence is evidence that directly proves a fact in issue, such as an Original document or a witness testimony. Primary evidence would include original financial and accounting records, as well as witness testimony from individuals involved in the financial transactions being audited.

Secondary Evidence is evidence that is used to prove the contents of a document or statement, such as a photocopy or a transcript, computer-generated reports, or other records that are used to support the findings of the audit.

In addition to primary and secondary evidence, the Act also recognises the concept of "opinion evidence," which refers to evidence given by an expert witness who is qualified to provide an opinion on a particular matter. In a forensic audit, an expert witness might be called upon to provide an opinion on the authenticity of financial records or to explain complex financial transactions to the court.

In the case of forensic audits, the reports generated by the forensic auditor can be considered as documentary evidence and can be admitted in court as evidence under certain conditions.

In the context of forensic audits, the Act is relevant in determining what types of evidence can be used to support the findings of the audit. The Act defines what constitutes evidence, how evidence should be presented, and what type of evidence is admissible in a court of law.

In addition to the Act, the Institute of Chartered Accountants of India (ICAI) has issued Standards for doing forensic accounting and investigation (FAIS). These guidelines cover the principles and practices of forensic accounting and audit, the role of the forensic accountant or auditor, and the procedures for conducting a forensic audit.

The admissibility of forensic audit reports as evidence in Indian courts is determined by the Act, which requires that the evidence be relevant, reliable, and authenticated. The forensic auditor must have a thorough understanding of the Act and the rules of evidence to ensure that the various evidences gathered is admissible in court.

The Act also defines the burden of proof in a case, which is the responsibility of the party bringing the case to prove their case. The burden of proof can shift from one party to the other during the course of a trial, depending on the evidence presented.

Overall, the Indian Evidence Act plays a crucial role in ensuring that evidence presented in Indian courts is reliable, admissible, and relevant to the case at hand. It is an essential tool in the administration of justice in India.

In conclusion, forensic audits have become an essential tool in detecting and investigating financial fraud and white-collar crimes in India. However, the admissibility of forensic audit reports in court is subject to the rules of evidence under the Indian Evidence Act, 1872.

FINDING FACTS

Meaning of Fact

As per Oxford Learner's Dictionary- "a thing that is known to be true, especially when it can be proved."

As per Section 3 of the Indian Evidence Act, 1872, "Fact" means and includes

(1) Anything, state of things, or relation of things, capable of being perceived by the senses;

(2) Any mental condition of which any person is conscious.

Example

(a) That there are certain objects arranged in a certain order in a certain place, is a fact.

(b) That a man heard or saw something, is a fact.

(c) That a man said certain words, is a fact.

(d) That a man holds a certain opinion, has a certain intention, acts in good faith or fraudulently, or uses a particular word in a particular sense, or is or was at a specified time conscious of a particular sensation, is a fact.

(e) That a man has a certain reputation, is a fact.

Fact sometimes refers to that which is **adduced** by a party at the trial as a means of establishing factual claims. ("Adducing evidence" is the legal term for presenting or producing evidence in court for the purpose of establishing proof.)

As per Section 3(2) (e) of the Act, "A fact is said to be proved when, after considering the matters before it, the Court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists".

"Disproved"- A fact is said to be disproved when, after considering the matters before it, the Court either believes that it does not exist, or considers its non-existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it does not exist.

"Not proved" - A fact is said not to be proved when it is neither proved nor disproved.

"To be relevant the evidence need merely have some tendency in logic and common sense to advance the proposition in issue".

"any two facts to which [relevance] is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other".

Evidence under the Act

As per Section 3 of the Act, "Evidence" means and includes:

1. all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;
2. all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.

Evidence can be anything presented to the five senses (sight, smell, hearing, taste and touch) including testimony, documents and material objects.

Evidence is divided into three main categories:

1. Oral evidence (the testimony given in court by witnesses),
2. Documentary evidence (documents produced for inspection by the court), and
3. "Real evidence".

Oral evidence and documentary evidences are self-explanatory and real evidence captures things other than documents such as a knife allegedly used in committing a crime, finger prints found at the crime scene etc.

The term "evidence" can refer to a proposition of fact that is established by evidence in the first sense. This is sometimes called an "evidential fact". That the accused was at or about the scene of the crime at the relevant time is evidence in the second sense of his possible involvement in the crime.

But the accused's presence must be proved by producing evidence in the first sense. For example, the prosecution may call a witness to appear before the court and get him to testify that he or she saw the accused in the vicinity of the crime at the relevant time. Success in proving the presence of the accused (the evidential fact) depends on the fact-finder's assessment of the veracity of the witness and the reliability of his or her testimony.

The fact-finder is the person or body responsible for ascertaining where the truth lies on disputed questions of fact and in whom the power to decide on the verdict vests. The fact-finder is also called "trier of fact" or "judge of fact".

Fact-finding is the task of the jury or, for certain types of cases and in countries without a jury system, the judge.) Sometimes the evidential fact is directly accessible to the fact-finder. If the alleged knife used in committing the crime in question (a form of "real evidence") is produced in court, the fact-finder can see for himself the shape and size of the knife; he does not need to learn of it through the testimony of an intermediary.

A third conception of evidence is an elaboration or extension of the second. On this conception, evidence is relational. A factual proposition (in Latin, factum probans) is evidence in the third sense only if it can serve as a premise for drawing an inference (directly or indirectly) to a matter that is material to the case (*factum probandum*).

The fact that the accused's fingerprints were found in a room where something was stolen is evidence in the present sense because one can infer from this that he was in the room, and his presence in the room is evidence

of his possible involvement in the theft. On the other hand, the fact that the accused's favorite colour is blue would, in the absence of highly unusual circumstances, be rejected as evidence of his guilt: ordinarily, what a person's favorite colour cannot serve as a premise for any reasonable inference towards his or her commission of a crime and, as such, it is irrelevant.

Suppose if it emerges during cross-examination of the finger print expert that his testimony of having found a finger-print match was a lie. Lawyers would describe this situation as one where the "evidence" (the testimony of the expert) fails to prove the fact that it was originally produced to prove and not that no "evidence" was adduced on the matter.

Here "evidence" is used in the first sense—evidence as testimony—and the testimony remains in the court's record whether it is believed or not. But lawyers would also say that, in the circumstances, there is no "evidence" or proof that the accused was in the room, assuming that there was nothing apart from the discredited expert testimony of a fingerprint match to establish his presence there.

Here, the expert's testimony is shown to be false and fails to establish that the accused's fingerprints were found in the room, and there is no (other) factual basis for believing that he was in the room. The factual premise from which an inference is sought to be drawn towards the accused's guilt is not established.

Fourthly, the conditions for something to be received (or, in technical term "admitted") as evidence at the trial are sometimes included in the legal concept of evidence. On this conception, legal evidence is that which counts as evidence in law. Something may ordinarily be treated as evidence and yet be rejected by the court. Hearsay is often cited as an example. It is pointed out that reliance on hearsay is a commonplace in ordinary life. We frequently rely on hearsay in forming our factual beliefs.

In contrast, "hearsay is not evidence" in legal proceedings. As a general rule, the court will not rely on hearsay as a premise for an inference towards the truth of what is asserted. It will not allow a witness to testify in court that another person X (who is not brought before the court) said that on a certain occasion (an out-of-court statement).

In summary, at least four possible conceptions of legal evidence are in vogue:

i. As an object of sensory evidence,

ii. as a fact,

iii. as an inferential premise, and

iv. as that which counts as evidence in law.

The sense in which the term "evidence" is being used is rarely made explicit in legal discourse although the intended meaning will often be clear from the context.

QUESTION OF FACT

In law, a question of fact, also known as a point of fact, is a question that must be answered by reference to facts and evidence as well as inferences arising from those facts. Such a question is distinct from a question of law, which must be answered by applying relevant legal principles. The answer to a question of fact (a "finding of fact") usually depends on particular circumstances or factual situations.

All questions of fact are capable of proof or disproof by reference to a certain standard of proof. Depending on the nature of the matter, the standard of proof may require that a fact be proven to be "more likely than not" (there is barely more evidence for the fact than against, as established by a multitude of the evidence) or true beyond reasonable doubt.

Answers to questions of fact are determined, by a trier of fact such as a jury, or a judge.

In many jurisdictions, appellate courts generally do not consider appeals based on errors of fact (errors in answering a question of fact). Rather, the findings of fact of the first venue are usually given great high opinion by appellate courts.

QUESTION OF LAW

A question of law, also known as a point of law, is a question that must be answered by applying relevant legal principles to interpretation of the law. Such a question is distinct from a question of fact, which must be answered by reference to facts and evidence as well as inferences arising from those facts. Answers to questions of law are generally expressed in terms of broad legal principles and can be applied to many situations rather than be dependent on particular circumstances or factual situations.

An answer to a question of law as applied to the particular facts of a case is often referred to as a "conclusion of law." In several civil law jurisdictions, the highest courts consider questions of fact settled by the lower court and will only consider questions of law. They thus may refer a case back to a lower court to re-apply the law and answer any fact-based evaluations based on their answer on the application of the law.

International courts will only answer questions of law, asked by judges of national courts if they are not certain about the interpretation of the law of multilateral organizations. While questions of fact are resolved by a trier of fact, which in the common law system is often a jury, questions of law are always resolved by a judge or equivalent. Whereas findings of fact in a common law legal system are rarely overturned by an appellate court, conclusions of law are more readily reconsidered.

TYPES OF EVIDENCES

Direct Evidence: It proves a fact directly and includes testimony that tends to prove or disprove a fact. A video tape captured by CCTV in the factory showing James taking high value item by entering the warehouse and clandestinely carrying it out of the factory is a direct evidence and it is compelling.

Circumstantial Evidence: It tends to prove or disprove a fact in issue indirectly by inference. If we go to bed at night and at that time there is no wetness on the ground and the next morning there is wetness on the ground, this is circumstantial evidence that it rained last night. Many fraud cases are proved entirely by circumstantial evidence, or by a combination of circumstantial and direct evidence, but seldom by direct evidence alone.

MEANING OF RELEVANT FACTS

In India, which is a common law country, we follow adversarial system of law. Judges do not question the parties and merely rely on evidence put forth by them. From such evidences, judges infer actual circumstances and therefore come to truth and deliver justice.

"Relevant" - One fact is said to be relevant to another when the one is connected with the other in any of the ways referred to in the provisions of this Act relating to the relevancy of facts.

As per Section 3 of the Act,

The expression "facts in issue" means and includes –– any fact from which, either by itself or in connection with other facts, the existence, non-existence, nature or extent of any right, liability, or disability, asserted or denied in any suit or proceeding, necessarily follows.

Whenever, under the provisions of the law for the time being in force relating to Civil Procedure any Court records an issue of fact, the fact to be asserted or denied in the answer to such issue is a fact in issue.

Example:

A is accused of the stealing inventory of B Limited.

At this trial the following facts may be in issue:-

That A stole B Limited's inventory;

That A intended to steal B Limited's inventory.

As per Section 5 of the Act, Evidence may be given of facts in issue and relevant facts. Evidence may be given in any suit or proceeding of the existence of non-existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others. This section shall not enable any person to give evidence of a fact which he is disentitled to prove by any provision of the law for the time being in force relating to Civil Procedure.

As per Section 6 of the Act, Relevancy of facts forming part of same transaction. Facts which, though not in issue, are so connected with a fact in issue as to form part of the same transaction, are relevant, whether they occurred at the same time and place or at different times and places.

Example:

The question was, whether A stole inventory from B Ltd. The facts that, shortly after stealing, A went out of the factory with inventory in his possession, and that was captured in CCTV are relevant.

As per Section 8 of the Act, Any fact is relevant which shows or constitutes a motive or preparation for any fact in issue or relevant fact. The conduct of any party, or of any agent to any party, to any suit or proceeding, in reference to such suit or proceeding, or in reference to any fact in issue therein or relevant thereto, and the conduct of any person an offence against whom is the subject of any proceeding, is relevant, if such conduct influences or is influenced by any fact in issue or relevant fact, and whether it was previous or subsequent thereto.

Explanation 1

The word "conduct" in this section does not include statements, unless those statements accompany and explain acts other than statements; but this explanation is not to affect the relevancy of statements under any other section of this Act.

Explanation 2

When the conduct of any person is relevant, any statement made to him or in his presence and hearing, which affects such conduct, is relevant.

Example:

A sues B upon a promissory note for the payment of money, B denies the making of the promissory note. The fact that, at the time when the promissory note was alleged to be made, B required money for a particular purpose, is relevant.

As per Section 9 of the Act: Facts necessary to explain or introduce relevant facts.

A, accused of theft, is seen to give the stolen property to B, who is seen to give it to A's wife.

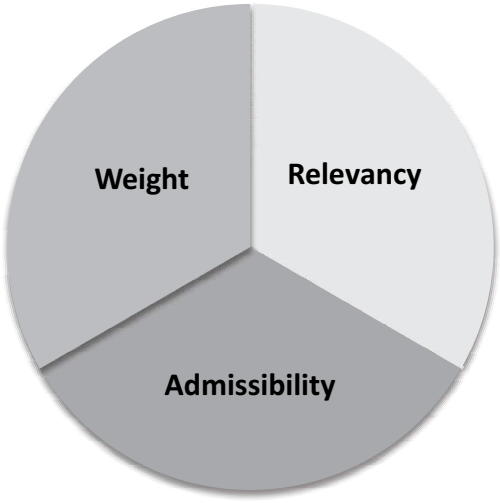
B says as he delivers it– "A says you are to hide this."

B's statement is relevant as explanatory of a fact which is part of the transaction.

Whether a particular piece of evidence is relevant or not depends on what the evidence is offered to prove. An item of evidence might be relevant and admissible if offered to prove one thing, but not relevant and inadmissible if offered to prove something else.

Evidence would be admissible if offered to prove motive, intent, identity, absence of mistake, or modus operandi, if such factors are at issue.

For an evidence to have any value in the eyes of court of law and be relied upon on reaching the decision these few rules have to be kept in mind:



1. Relevancy;
2. Admissibility; and
3. Weight.

Relevancy

There are two important ingredients:

1. **Material connection (or relation to fact in issue or another fact.):** It means that the fact in issue and the fact to be produced must have some sort of connection or they should be related to each other. Something cannot exist without any reason. The state of one thing affects the formulation of another and thus the material connection defines that relation, effect, cause or reasoning.
2. **Probative value:** Probative means 'capacity to prove something'. A relevant fact must 'prove' or 'render probable' the existence or non- existence of fact in issue or other fact. It implies that either something is proved beyond doubt or the probability that something exists has grown higher by producing the evidence.

CASE STUDY

Who is the culprit?

A, B and C are very good friends who trust each other a lot and often visit each other. C is kleptomaniac. He comes to visit A at his home along with B. All the three had dinner together. All of them discussed about cricket match going on. After B and C left, A suddenly finds that his i-Phone is missing. Now the question comes who has stolen it? The discussion about cricket match is not anyway related to the fact of missing mobile phone. The visit of both B and C is material. But it does not prove or make probable anything as they often visit A.

Also, the fact that C is kleptomaniac and possesses special interest in stealing high value mobile phone is material to show that he might have interest. It also makes it more probable that he has stolen and not B. Thus the fact of C being kleptomaniac is material and makes his guilt more probable.

Tests to determine Relevancy

Often it becomes difficult to draw a line between relevant and irrelevant material. In such circumstances it becomes necessary to lay down test of relevancy. The test can be considered by also having a look at two types of relevancy.

Logical Relevancy:

The reliance is to be proved on common stock of knowledge about the world that is logic, common sense and general experience. Thus when we derive relevancy on the basis of logic it can be said logical relevancy. There are many ways to derive relevancy on the basis of logic. For example syllogism. A syllogism is a type of logical reasoning where the conclusion is gotten from two linked premises.

- An apple is a fruit. All fruit is good. Therefore apples are good.
- All Thieves are Criminals; A is a Thief; Therefore, A is a Criminal.

But, Logical relevance is not necessarily be admissible in the court of law. If the legislature lays down guidelines to test relevancy then such guidelines will prevail over logical reasoning.

Legal Relevancy*:*

By legal relevancy it means that a fact should be relevant under the rules laid down by law. In India Section 5 of the Act, provides that only those evidences can be given which are relevant under the Act. (Section 6 to 55). Hence, these provisions lay down what are the relevant facts to be considered while recording evidences. Any fact howsoever material not falling under the provisions will not be considered as evidence and hence not admissible. Thus, the actual test to determine relevancy becomes whether the fact is relevant under the provisions of the statute or not.

Admissibility and Weight of an Evidence

The court after deciding whether the fact is relevant or not decides upon the matter of admissibility. By admissibility it means capability to be accepted. A fact may be highly relevant but to the disappointment of lawyer court may refuse to admit the evidence because it is non-admissible for several reasons. Thus if an evidence is legally relevant and does not prejudice the trial then only it will be admissible in the court of law. Whether evidence outweighs costs of admission depends on the discretion of the court. Thus if admission has an adverse effect on the course of fair proceeding the court will not admit it.

That is, if admission of an evidence misleads a jury or causes undue delay in the proceedings or proves an already established fact then such an evidence will be rejected. Normally a trial judge would first determine the logical relevance of evidence and then weighs its potential probative value against the possible costs of admissions.

The above mentioned rules were to be decided by the jury or the trial judge. They used to have large discretion for admitting evidence on record. However, in India the Evidence Act, 1872 lays down in detail all the tests of relevancy and admissibility of the facts to determine a fact in issue and pronounce the judgment. The Act has incorporated in itself all these rules thereby narrowing down the scope for discretion of judges.

ADMISSION OF EVIDENCE

Every case, whether civil or criminal, that comes before a court of law has a fact story behind it. Facts out of which cases arise keep happening in the ordinary course of life.

To illustrate, imagine that there is a crowded road and it is Monday morning, people are moving, and vehicles are moving. Everyone is running at unmitigated speed, suddenly two vehicles collide against each other. The nature and cause of the accident would be in question. The facts which led up to the climax will have to be reconstructed before the court, so that the judge in the court is able to consider what really happened. Only then he will be able to apply the appropriate law to the fact to arrive at a solution about the right and liabilities of the parties.

The practical reality is that the truth of a case is worthless unless they can be proved to the satisfaction of the judge and allows him to act on them. The means by which facts are proved are governed by the law of evidence.

The function of the law of evidence is laid down rules according to which the facts of case can be proved or disproved before a court of law. The means which can be used to prove a fact are all controlled by the rules and principles lay down by the law of evidence. The law of evidence does not affect substantive right of parties but only lays down the law for facilitating the rules of evidence for the purposes of the guidance of the court.

It is procedural law which provides how a fact is to be proved. The evidence means, any things by which any alleged matter of facts is either established or disproved. Evidence is of many kinds and one of the important ones is 'Admission'.

Admission

Admission is a voluntary acknowledgment of a fact. Importance is given to those admissions that go against the interests of the person making the admission. This concept is governed by the rules and regulations mentioned under Indian Evidence Act, 1872, Section 17-23.

For example, when A says to B that he stole money from C, A makes an admission of the fact that A stole money from C. This fact is detrimental to the interests of A. The concept behind this is that nobody would accept or acknowledge a fact that goes against their interest unless it is indeed true.

Unless A indeed stole money from C, it is not normal for A to say that he stole money from C. Therefore, an admission becomes an important piece of evidence against a person.

On the other hand, anybody can make assertions in favor of themselves. They can be true or false. For example, A can keep on saying that a certain house belongs to himself, but that does not mean it is necessarily true. Therefore, such assertions do not have much evidentiary value.

An admission is any statement made by a party to a lawsuit (either before a court action or during it) which tends to support the position of the other side or diminish his own position. For example, if a husband sues his wife for divorce on the grounds of adultery, and she states out of court that she has had affairs, her statement is an admission.

Any admission made by a party is admissible evidence in a court proceeding, even though it is technically considered hearsay (which is normally inadmissible). Attorneys tell their clients not to talk to anyone about their case or about the events leading up to it in order to prevent their clients from making admissions.

An admission is the testimony which the party admitting bears to the truth of a fact against himself. It is a voluntary act, which he acknowledges as true the fact in dispute. An admission and consent is, in fact, one and the same thing, unless indeed for more exactness we say, that consent is given to a present fact or agreement, and admission has reference to an agreement or a fact anterior for properly speaking, it is not the admission which forms a contract, obligation or engagement, against the party admitting. The admission is, by its nature, only the proof of a pre-existing obligation, resulting from the agreement or the fact, the truth of which is acknowledged.

Section 17 - "An admission is a statement, oral or documentary or contained in electronic form, which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned."

An admission is a statement of fact which waives or dispenses with the production of evidence by conceding that the fact asserted by the opponent is true.

Admissions are admitted because the conduct of a party to a proceeding, in respect to the matter in dispute, whether by acts, speech or writing, which is clearly inconsistent with the truth of his contention, is a fact relevant to the issue. Admissions are very weak kind of evidence and the Court may reject them if it is satisfied from other circumstances that they are untrue. *Ref: Latafat Husain v. Lala Onkar Mal (1934) 10 Luck 371.*

The Supreme Court has observed: Admissions as defined in Sections 17 and 20 and fulfilling the requirements of Section 21 are substantive evidence. An admission is the best evidence against the party making it and, though not conclusive, shifts the onus to the maker on the principle that what a party himself admits to be true may be reasonable presumed to be true so that until the presumption is rebutted the fact admitted must be taken to be true. *Ref: Thiru John v. Returning Officer, AIR 1977 SC 1724.*

Admissions made in several documents ante litem motam--Burden of proof shifts on the maker to show that they are erroneous. From the evidence on record it stood clearly established that on the date of the scrutiny of nominations Sri John was less than 30 years of age and in view of Article. 84(b) of the Constitution he was not competent to contest the election for the Rajya Sabha.

An assessee cannot resile from his admission made in tax return even at appellate stage. *Ref: Federal Bank Ltd. v. State, AIR 1995 Ker 62.*

Subject to certain exceptions, the general rule, both in civil and criminal cases, is that any relevant statement made by a party is evidence against himself. The weight of the declaration is, of course, a totally different matter; this may vary with the circumstances and will not doubt, be greater if against interest at the time, than the contrary"

An admission is defined in Section 17, Indian Evidence Act, 1872, as a statement, oral or documentary, which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons and under the circumstances mentioned in the three succeeding sections.

The section does not, therefore, contain a complete definition of the word "admission", in as much as it does not define the persons whose statements amount to admissions, nor the circumstances under which a statement must be made so that it may amount to an admission.

This part of the definition of an admission is left to sections 18-20. Therefore, the question whether a statement amounts to an admission or not depends upon whether it was made by any of the persons, and in any of the circumstances, described in sections 18-20, and whether it suggests an inference as to a fact in issue or a relevant fact in the case.

The fact that the statement suggests an inference in favor of the person who made the statement does not make the statement any the less an admission, as the question whether a statement is or is not an admission different from the question whether an admission may or may not be proved in favor of the person making it.

A statement may be an "admission" in the sense in which this word is used in this set of sections, it must be an oral or documentary statement. A statement may be made otherwise than by word of mouth or writing but such a statement can hardly be described as an oral or documentary statement. *Ref: Brij Nandan v. Emperor., 133 IC 154: 1931 A 9: 32 Cr LJ 1006.*

Admissions by conduct are not governed by this set of sections, as inferences suggested by active or passive conduct are not oral or documentary statements. The proper section under which the relevancy of admissions by conduct must be established is the Section 8 of the Act, as a statement made by conduct will be admissible or inadmissible according to whether it falls or does not fall within the terms of that section.

An admission must be used either as a whole or not at all. *Ref: Hanumant Govind Nargundkar v. State of Madhya Pradesh, 1952 SCR 1091.*

When a statement which is sought to be given in evidence forms part of a longer statement, evidence shall be given of so much of the statement as is necessary to the full understanding of the nature and effect of the statement. Section 39 of Indian Evidence Act, 1872.

Before any statement can be used as an admission, it must be shown to be unambiguous and clear on the point at issue. *Ref: Paresh Nath v. Ghasi Ram, AIR 1960 Pat 407.*

If an admission is capable of two interpretations, an interpretation unfavorable to the person making it should not be put on his admission. The requirement is that an admission must be clear, precise, not vague or ambigious. *Ref: C. Koteshwara Rao v. C. Subbarao, AIR 1971 SC 1542.*

When an admission is intended to be relied upon, the admission must be regularly proved. *Ref: Moni Lal Kar Chowdhry v. Uma Charan Chakravarty, 25 IC 571: 19 Cr LJ 541.*

An admission may be proved in any of the ways in which a statement is permitted to be proved. The person who made the admission may be called and questioned as to his having made the alleged admission, or any person in whose presence the statement was made may be called and examined.

If the admission is contained in a document, the document must be proved in any of the ways in which a document is provable.

An admission contained in a plaint must be proved in one of the ways in which a statement contained in a document may be proved; and since a plaint is not a public document a certified copy of it is not the proper proof of an admission contained in it. *Ref: Ahmad Khan v. Hurmuzi Khanam, 61 IC 117*

Section 18 postulates that statements made by a party to the proceeding or by an agent to any such party, whom the Court regards, under the circumstances of the case as expressly or impliedly authorized by him to make them, are admissions.

Equally: statement made by a person who has any proprietary or pecuniary interest in the subject matter of the proceedings or by persons having derivative interest during the continuance of the interest also is admissions. *Ref: Shrichand Gupta v. Gulzar Singh, AIR 1992 SC 123*

Where a party sues or is sued in a representative capacity, e.g. as trustee, executor, administrator or the like, his representative capacity is distinct from his ordinary capacity, and only admissions made in the former capacity are receivable whereas statements made before he acquired the representative character are inadmissible. *Ref: Sena Yasim Sahib v. Kadur Ekambara Iyer, 54 IC 497*

Thus, an admission by the trustee of a bankrupt, made before he acquired the character of a trustee, is not receivable against him when he is sued as a trustee. *Ref: Fenwick v. Thornton, (1827) M&M 51*

Conversely, an admission by a person in his representative capacity is not receivable against him as a party in his personal capacity.

Section 19 - Admissions by persons whose position must be proved as against party to suit- Statements made by persons whose position or liability it is necessary to prove as against any party to the suit, are admissions, if such statements would be relevant as against such persons in relation to such position or liability in a suit brought by or against the made if they are made whilst the person making them occupies such position or is subject of such liability.

The admissions of a bankrupt before the act of bankruptcy are receivable in proof of the petitioning creditors' debts. A statement made by a servant is admissible in evidence against his master under section 19, both for

the purpose of deciding whether he is a servant and also as regards his liability as such servant. "Occupying the position" of a servant does not involve, as an essential ingredient, acting in the course of his employment. *Ref: M.E. Moses v. Shaik Bakridhone Chowdhury, 39 CWN 736*

Section 20 - Admission by persons expressly referred to by party to suit - Statements made by persons to whom a party to the suit has expressly referred for information in reference to a matter in dispute are admissions.

This section forms another exception to the rule that admissions by strangers to a suit are not relevant. Under it, the admissions of a third person are also receivable in evidence against, and have frequently been held to be in fact binding upon, the party who has expressly referred another to him for information in regard to an uncertain or disputed matter.

Section 21 - Admissions are relevant and may be proved as against the person who makes them or his representative in interest; but they cannot be proved by or on behalf of the person who makes them or by his representative in interest, except in the following cases: –

(1) An admission may be proved by or on behalf of the person making it, when it is of such a nature that, if the person making it were dead, it would be relevant as between third persons under section 32.

(2) An admission may by proved by or on behalf of the person making it, when it consists of a statement of the existence of any state of mind or body, relevant or in issue, made at or about the time when such state of mind or body existed, and is accompanied by conduct rendering its falsehood improbable.

(3) An admission may be proved by on behalf of the person making it, if it is relevant otherwise than as an admission.

As a general rule, a man shall not be allowed to make, evidence for himself. But on the other hand, universal experience testifies that, as men consult their own interest and seek their own advantage, whatever they say or admit against their interest or advantage may, with tolerable safety, be taken to be true as against them, at least until the contrary appears. Refer Section 21 of the Act.

The question between A and B is whether a certain deed is or is not forged. A affirms that deed is genuine, B states that it is forged. A may prove a statement by B that the deed is genuine, and B may prove a statement by A that deed is forged; but A cannot prove a statement by himself that the deed is genuine, nor can B prove a statement by himself that the deed is forged.

Section 22 - Oral admissions as to contents of a document are excluded under Section 22 of the Act. They are, however, admissible when the party is entitled to give secondary evidence of the contents of such document under Section 65 and 66. Such admissions are also admissible when the genuineness of the document produced is in question.

As to the validity of a gift deed, one of the donors stated that he was a minor at the time of its execution. But in the gift deed itself he admitted his age to be 22. This admission was contained in the registered deed. This was held to be binding on him unless he could show any vitiating circumstance like fraud, coercion etc. *Ref: Patel Prabhudas Hargovandas v. Heirs of Patel Babubhai Kachrabhai, AIR 2007 Guj 148.*

Section 22A – Oral admission as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

Section 22A of the Act has been inserted due to introduction of Information Technology Act, 2000.

The purpose of this section is to provide for the circumstances in which an oral admission could be proved as to the contents of an electronic record. The section disallows the evidence of oral admission as to the contents of an electronic record. It talks of an exceptional situation, which is that when the genuineness of the electronic record produced before the court is itself in question. The section says that oral admissions as to the contents of an electronic record may be proved in evidence when the genuineness of the record has been questioned.

Section 23 - In civil cases no admission is relevant, if it is made either upon an express condition that evidence of it is not to be given, or under circumstances from which the Court can infer that the parties agreed together that evidence of it should not be given.

Section 23 of the Act is applicable to civil as well as to criminal cases. It consists of two distinct parts. Under the first part, an admission is not admissible in evidence, if it is made on the express condition that it is not to be given in evidence. If the admission is not made upon such condition, but the Court can infer that the person making the admission and the party to whom the admission was made had agreed that the admission would not be given in evidence, the admission thus made will be inadmissible under the second part of the section.

Where an admission is made upon a condition that it is not to be given in evidence, it is usual, though not necessary, to describe it as "without prejudice". Thus, where the plaintiff, to save limitation, relied upon a post card written by the defendant «without prejudice," in which he promised to pay Rs.XXX and acknowledged his liability to pay any sum that may be due, the post card was held to be inadmissible in evidence under this section. *Ref: Madhavrav Ganeshpant Oze v. Gulabbhai Lallubhai, 23 B 177*

An offer, made by the Government "without prejudice" to pay a certain amount for acquisition of land under the Land Acquisition Act is not admissible in evidence. *Ref: Ranzor Singh v. Secretary of State, 92 IC 319: 1926 L 509*

It has been held in an Oudh case that a letter written "without prejudice" is not admissible in evidence as it merely shows a desire on the part of the writer to have the privilege, and not an agreement on the part of the other party to respect the privilege. *Ref: Lucknow Improvement Trust v. Jaitly & Co., 5 Luck 465*

But, it is submitted that such letter would be inadmissible under the first part of the section, as it amounts to an admission upon an express condition that it is not to be given in evidence.

An admission contained in a draft of a compromise deed filed in Court must be excluded where the document provides that the parties to it would be free to repudiate any condition of the proposed compromise by which, in their opinion, their rights were prejudicially affected. *Ref: Surendra Prasad Lahiri v. Gobinda Das, 48 CWN 15.*

METHODS TO PROVE CASES

As per Section 3 of the Act, "Evidence". ––"Evidence" means and includes ––

1. All statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;
2. All documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.

Evidence can be anything presented to the five senses (sight, smell, hearing, taste and touch) including testimony, documents and material objects.

Evidence is basically of two types- Oral Evidence and Documentary Evidence. These have been explained in detail below:

Oral Evidence

As per Section 3 of the Act, it means statements which the Court permits or requires to be made before it by witnesses in relation to matter of fact under inquiry.

As an Evidence, Oral evidence is as much less satisfactory medium of proof than documentary evidence. But however fallible such evidence may be and however carefully it may have to be watched, justice can never be administered in the most important cases without recourse to it.

Oral evidence is generally is not subject to rule of presumption and is judged with reference to the conduct of the parties.

It means - false in one particular, false in all.

This principle has no application in India. Even if major portion of evidence is found to be deficient, still residue is sufficient to prove guilt of an accused, notwithstanding acquitted of number of other co-accused persons. In Gangadhar Behera vs. State of Orissa. It has been held that the maxim "falsus in uno falsus in omnibus" has no application in India and the witnesses cannot be branded as liar. This maxim is merely a rule of caution.

In Sucha Singh v. State of Punjab, it has been held this maxim has no application in India. The Supreme Court has even observed that "the principle of Falsus in uno falsus in omnibus does not apply to criminal trials and it is the duty of the court to separate, the grain from the chaff instead of rejecting the prosecution case on general grounds. *Ref: BheRam v. State of Haryana, AIR (1980) 1 SCC 201*

Appreciation of Oral Evidence Oral evidence should be approached with caution. Following are among the most important points to be ascertained in deciding on the credibility of witnesses:

a) Whether they have the means of gaining correct information;

b) Whether they have any interest in concealing truth; and

c) Whether they agree in their testimony.

The credibility of a witness is primarily to be decided by referring to his evidence and finding out as to how the witness was found in the cross-examination and what impression is created by his evidence taken in context of the other facts of the case.

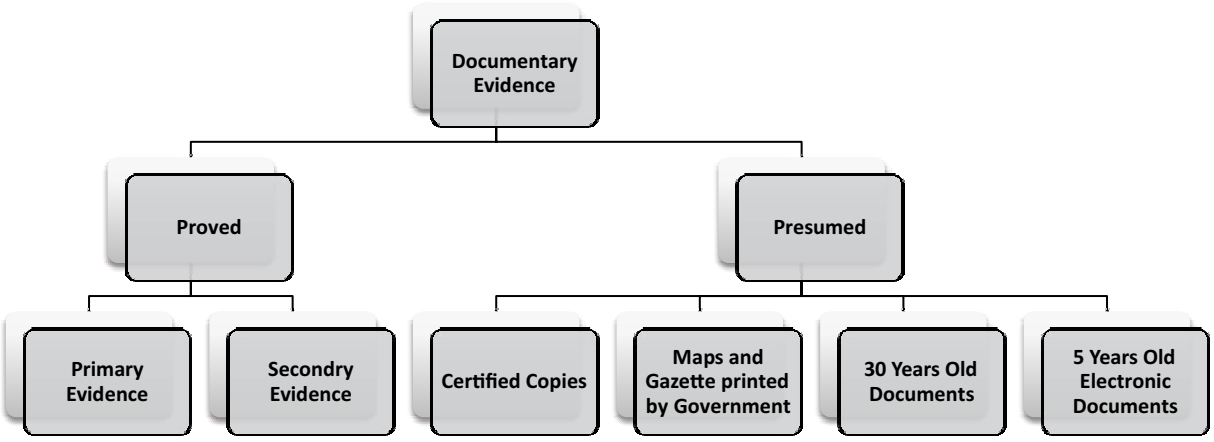
In *State of Bihar* v. *Radha Krishna Singh, AIR 1983 SC 684* the Supreme Court observed: "in considering the oral evidence regarding a pedigree a purely mathematical approach cannot be made because where a long line of descent has to be proved spreading over a century.

Section 60 of Evidence Act requires that the oral evidence must, in all cases whatsoever, be direct. Where the testimony of the witness is entirely hearsay and on some matters hearsay of hearsay, it cannot be admitted in evidence. Where a witness gives evidence that he received information from other person and that person does not say about it, such evidence would be inadmissible being hearsay evidence. *Ref: Kirtan Prasad v. State of Madhya Pradesh, 2005 Cr LJ 69 MP.*

Rejection of Hearsay Evidence

The reasons that hearsay evidence is treated as untrustworthy are that the original declare ant of the statement which is offered in a second hand manner is not put on oath, nor is he subject to cross-examination, and the accused, against whom, such evidence is offered, loses his opportunity of examining into the means of knowledge of the original maker of the statement, the truth of the original statement is diminished in course of repetition of that statement, that admissibility of hearsay evidence would open up opportunities of weaker for stronger proof regarding proof of a fact in issue or a relevant fact. *Ref: Herbetus Oram v. State, (1971) 37 CLT 477.*

Documentary Evidence



Meaning under Section 3 of the Evidence Act, all documents including electronic records produced for the inspection of the Court together constitutes to be documentary evidence.

The word 'Document' is again defined under Section 3 as- 'any matter expressed or described upon any substance by means of letter, figures or makes, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.'

1. Proof of document by primary or secondary evidence
2. Public and Private Documents
3. Presumptions of the various documents.

Proof by Primary and Secondary Evidence

The content of the document will be taken as evidence only when it is proved by some primary or secondary evidence. Section 61 read with section 64 and 65

Primary evidence means documents presented in the Court itself for examination.

Explanation I of Section 62 states that- Where a document is executed in counterparts, each part is primary evidence against the executing party and his privies; but, as against the non-executing party and his privies, it is only secondary evidence.

Explanation II states that- Printed, lithographic, photographic and other reproductions made by one uniform process are primary evidence of each other, but if, in the circumstances of a particular case, the original be not a reproduction but the document from which the reproduction was made, the reproduction would be merely secondary evidence of the original.

For instance, if it is desired to prove the publication of a libel in a newspaper, any copy of the issue in which libel appeared would be primary evidence of the publication in all the other copies of that issue. But if it were necessary to prove the original libel from which the article was set up, the printed paper would not be primary, but only secondary, evidence of the manuscript and admissible only under the conditions, which render the reception of secondary evidence admissible. *Ref: Prithi Chand v. State of Himachal Pradesh, AIR 1989 SC 702*

In the latter case there is no more guarantee of a printed copy being a true copy than of a written copy.

Section 64 of the Act makes it a rule to prove any document through primary evidence, unless they specifically fall under the category of documents to be proved by Secondary under Section 65.

Secondary Evidence

Section 63 of the Evidence Act defines the kinds of secondary evidence permitted by the Act; whereas section 65 defines the circumstances under which secondary evidence of the kind mentioned in Section 63 becomes admissible. Section 63 mentions five kinds of secondary evidences. It includes:

(1) Certified copies given under the provisions hereinafter contained;

(2) Copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies;

(3) Copies made from or compared with the original;

(4) Counterparts of documents as against the parties who did not execute them;

(5) Oral accounts of the contents of a document given by some person who has himself seen it.

The copy to be given in evidence must be proved to be a correct copy by the evidence of someone who can swear to its being a true copy. It is not necessary that the scribe of the copy should be produced. What is required to be proved is that the document produced is a true copy of the original. Copies of original documents would not be admissible in evidence when the originals were not produced at any time nor was any foundation laid for the establishment of the right to give secondary evidence. Ref: *Baidya Nath Dutt* v. *Kaminikant Gupta, 6 Cr LJ 572*.

Further, the Court in *Doerd Gilbert* v. *Ross*,held that if a party cannot produce original document, then an oral evidence of it can be given provided they are have some secondary evidence with them to prove the oral content.

Section 65 lays down the conditions, wherein specifically secondary evidences have to be given. It includes:

a) When the original is shown or appears to be in the possession or power of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;

b) When the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;

c) When the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;

d) When the original is of such a nature as not to be easily movable;

e) When the original is a public document within the meaning of section 74;

f) When the original is a document of which a certified copy is permitted by this Act, or by any other law in force in India to be given in evidence;

g) When the original consists of numerous accounts or other documents which cannot conveniently be examined in Court and the fact to be proved is the general result of the whole collection.

In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible.

In case (b), the written admission is admissible.

In case (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible.

In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents.

Under Section 67 of the Act, where a document is written by one person and signed by another, the handwriting of the former and the signature of the latter have both to be proved in view of the section. Thus, the basic idea is that the document must be proved before it is admitted in the Court. This has been upheld by the Court in *Abdool Ali* v. *Abdoor Rushman.*

Section 68 of the Act, further provides that if a document is required by law to be attested then it cannot be accepted as evidence unless attested. However, it would not be necessary to call the attesting witness as evidence in the Court. However, if in case of will, which requires attesting witness to be called as an evidence under Section 68, but the attesting witness could not be found then it needs to be proved that the signature of atleast one attesting witness must be in his handwriting and that the document must have been signed by the person in his writing.

However, section 70 and 71 of the Act says that if the attesting witness fails to recall of the attestation of such documents by him then the documents may be proved by other means. A record of the proceedings of a Court of Justice will be presumed to be genuine and accurate, if it is certified in the manner laid down in this section 86.

Private and Public Documents

Public Documents have been explained under Section 74 of the Evidence Act. It includes records of Sovereign Authority, tribunals and of public officers. Apart from these, all other documents constitute private documents under Section 75.

Such public documents may be produced as a proof of such documents by producing the certified copy, which has been certified by the public officer in control of such document, certifying them to be a true copy of the document.

Presumption of Documents

In general terms, presumption is an inference drawn from the contents of the document. Such presumption holds good unless they have been disproved by the other parties. The various kinds of presumptions have been explained under Section 4 of the Act.

Section 79 to 90 of the Act deals with the various types of presumption in evidences.

Section 79 says that the Court shall presume all certified copy to be evidence admissible in Court provided they have been certified in the manner prescribed by law.

Section 80 further provides that where any document is produced by the Evidence as part of his evidence, then such document, when accepted by the Court will qualify to be a part of the evidence so produced by the evidence and it shall be presumed that such evidence is genuine and the evidence in support of which it is presumed is also accepted in the Court.

Any maps, books or gazette printed and compiled by the Government are also presumed to be true under Section 81, 82 and 83. Section 85 presumes that every power-of-attorney made before a notary is also true.

Under Section 85A of the Act, the Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties. Any certified copy of foreign judicial record is also presumed to be a valid document under section 86.

If any telegraphic message is sent, then the Court shall make no presumption with regards to the person who has been given the message merely for the purpose of transmission.

The position is the same in case of electronic message under Section 88A. Here, the Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Section 90 of the Act deals with the resumption of documents which are 30 years old. It says that Where any document, purporting or proved to be thirty years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the signature and every other part of such document, which purports to be in the handwriting of any particular person, is in that person's handwriting, and, in the case of a document executed or attested, that it was duly executed and attested by the persons by whom it purports to be executed and attested.

Similar stand is taken for any electronic message which is 5 years old. It says that any such message is assumed to have been electronically signed by person or by someone authorized by him.

PROVING A MATTER THROUGH EVIDENCES ON THE BASIS OF SOURCES

Direct Evidence

Evidence is either direct or indirect. Direct Evidence is that evidence which is very important for the decision of the matter in issue. The main fact when it is presented by witnesses, things and witnesses is direct, evidence whereby main facts may be proved or established that is the evidence of person who had actually seen the crime being committed and has described the offence.

We need hardly point out that the evidence of the witness in Court is direct evidence as opposed to testimony to a fact suggesting guilt. The statement before the police only is called circumstantial evidence of, complicity and not direct evidence in the strict sense. It directly related to the real point in issue.

For example, testimony of an eye witness will be treated as a direct evidence. In another example if one person is alleging that another person has breached the terms of the agreement and hence he is liable to pay compensation to the first person in such category the original document of the agreement will constitute a direct evidence.

Direct evidence is considered to be superior to circumstantial evidence because it creates a direct nexus between the evidence and fact in question.

Circumstantial Evidence

There is no difference between circumstantial evidence and indirect evidence. Circumstantial Evidence attempts to prove the facts in issue by providing other facts and affords an instance as to its existence. It is that which relates to a series of other facts than the fact in issue but by experience have been found so associated with the fact in issue in relation of cause and effect that it leads to a satisfactory conclusion.

According to Justice Fetcher Monten the acceptance of evidence and there appreciation thereof is not a rigid mathematical formulae and hence the circumstantial evidence qualifies a significant role in any matter before the court to make it possible that the court should reach to truth, reality and actual happenings of the things.

According to Justice Stetson, circumstantial evidence is like a light in the dark which slowly touches all corners of a matter and bring the reality in front of the adjudicator. He further observes that circumstantial evidence has to be appreciated with utmost caution because if light is strong enough to remove all darkness then it will uplift the justice in the matter but if the light is weak and removes darkness from some part of the matter it may result into grave injustice to both the parties.

In modern times, circumstantial evidence are given importance. It is seen as an evidence which relates to the series of the facts other than the fact in issue. Circumstantial evidence assumes importance in both categories when either direct evidence is lacking or the direct evidence is not conclusive of the fact in issue.

In *Hanumant* v. *State of Madhya Pradesh*, The Hon'ble Supreme Court Observed, "In dealing with circumstantial evidence there is always the danger that suspicion may take the place of legal proof. It is important to remember

that in cases where the evidence is of a circumstantial nature the circumstances from which the conclusion of guilt is to be drawn should in the first instance, be fully established and all the facts so established should be consistent only with the hypothesis of the guilt of the accused.

In other words there can be a chain of evidence so far complete as not to leave any reasonable ground for a conclusion consistent with the innocence of the accused and it must be such as to show that within all human probability the act must have been done by the accused."

In *State of U.P.* v. *Ravindra Prakash Mittal* Supreme Court had taken a stron stand while redefining and reframing the evidentiary value of circumstantial evidence. Court said that circumstantial evidence. Court said that circumstantial evidence will be treated as a good piece of evidence if it qualifies the following tests:

a) The circumstances from which guilt is established must create a series of circumstances and must be fully proved.

b) The circumstances must be of conclusive nature and tendency.

c) Circumstantial evidence must not need any reasonable doubt regarding existence of fact.

d) It should create the hypothesis of guilt in such a way which includes all possibilities that only accused has committed the crime and it should exclude all possibilities that any person other than the accused has committed the crime.

Other kinds of Evidence

1. Real Evidence

Real Evidence means real or material evidence. Real evidence of a fact is brought to the knowledge of the court by inspection of a physical object and not by information derived from a witness or a document. Personal evidence is that which is afforded by human agents, either in way of disclosure or by voluntary sign. It indicates the object in proving or disproving the facts for which it is given in the court of law.

For example, contempt of court, conduct of the witness, behaviour of the parties, the local inspection by the court. It can also be called as the most satisfactory witness.

2. Expert Evidence

Section 45, 45A, 46 and 47 deal with expert evidence. It constitutes significant evidence in the court of law because it qualifies the test of reliability in the court of law. The expert evidence is considered to be reliable because an expert is having a much better knowledge in the specific area in comparison to other people outside that area.

For example, a legal professional will be a reliable source on the constitutionality of any provision in comparison to an engineer about the constitutional validity or invalidity of evidence in the court of law.

There are certain principles which make expert evidence admissible evidence in the court of law:

a) The expert must be qualified in that discipline.

b) The expert must be within the recognised field of his expertise.

c) The evidence of the expert should be supported by his reliable and logical contentions. d) The expert should have acquired an expertise in these matters by his continuous work and continuous practice in the particular field.

d) He has been duly channelized under the scheme of examination in the court of law.

3. Hearsay Evidence

Hearsay Evidence is very weak evidence. It is only the reported evidence of a witness which he has not seen either heard. Sometime it implies the saying of something which a person has heard others say.

In *Lim Yam Yong* v. *Lam Choon & Co.* The Hon'ble Bombay High Court adjudged "Hearsay Evidence which ought to have been rejected as irrelevant does not become admissible as against a party merely because his council fails to take objection when the evidence is tendered."

Hearsay Evidence is that evidence which the witness has neither personally seen nor heard, nor has he perceived through his senses and has come to know about it through some third person. There is no bar to receive hearsay evidence provided it has reasonable nexus and credibility.

When a piece of evidence is such that there is no prima facie assurance of its credibility, it would be most dangerous to act upon it. Hearsay evidence being evidence of that type has therefore, to be excluded whether or not the case in which its use comes in for question is governed by the Evidence Act.

4. Primary Evidence

Section 62 of The Indian Evidence Act says Primary Evidence is the top-Most class of evidences. It is that proof which in any possible condition gives the vital hint in a disputed fact and establishes through documentary evidence on the production of an original document for inspection by the court. It means the document itself produced for the inspection of the court. In *Lucas* v. *Williams Privy Council* held "Primary Evidence is evidence which the law requires to be given first and secondary evidence is the evidence which may be given in the absence of that better evidence when a proper explanation of its absence has been given."

5. Secondary Evidence

Section 63 says Secondary Evidence is the inferior evidence. It is an evidence that occupies a secondary position. It is such evidence that on the presentation of which it is felt that superior evidence yet remains to be produced. It is the evidence which is produced in the absence of the primary evidence therefore it is known as secondary evidence.

If in place of primary evidence secondary evidence is admitted without any objection at the proper time then the parties are precluded from raising the question that the document has not been proved by primary evidence but by secondary evidence.

But where there is no secondary evidence as contemplated by Section 66 of the Evidence Act then the document cannot be said to have been proved either by primary evidence or by secondary evidence."

6. Positive and Negative Evidence

Evidence was categorized as positive and negative in the case of *Rahim Khan* vs. *Khurshid Ahmad.*

Positive evidence is any evidence which claims the existence of a fact.

A negative evidence is an evidence that claims non-existence of a fact.

The distinction lies on the fact that they guide the court towards the approach they have to take. Evidence includes everything that is used to determine or demonstrate the truth of an assertion. Giving or procuring evidence is the process of using those things that are either (a) presumed to be true, or (b) which were proved by evidence, to demonstrate an assertion's truth.

Evidence is the currency by which one fulfills the burden of proof. In law, the production and presentation of evidence depends first on establishing on whom the burden of proof lays.

Admissible evidence is that which a court receives and considers for the purposes of deciding a particular case.

There are two primary burden-of-proof considerations exist in law.

The first is on whom the burden rests. In many, Western countries, the burden of proof is placed on the prosecution.

The second consideration is the degree of certainty proof must reach, depending on both the quantity and quality of evidence. These degrees are different for criminal and civil cases.

Criminal cases require evidence beyond reasonable, the civil cases considers only which side has the preponderance (multitude)of evidence, or whether the proposition is more likely true or false. The decision maker, often a jury, but sometimes a judge, decides whether the burden of proof has been fulfilled. After deciding who will carry the burden of proof, evidence is first gathered and then presented before the court.

PROCEDURE TO BE PERFORMED WHILE DOING FORENSIC AUDIT

Plan the Investigation

When the forensic auditor is appointed by any client (including statutory authorities) the auditor needs to understand the scope and focus first before starting the assignment.

Collect the Evidence

The forensic auditor is required to understand and identify the possible type of fraud that has been carried out in the organisation and how the fraud has been perpetrated. The evidence collection should be reliable and adequate to prove the charges and identify the fraudsters in court of law. Forensic auditor should reveal the details of fraud scheme with the help of evidence collected during the course of assignment. Forensic auditor should document the evidence to prove the amount of loss sustained, the parties directly and indirectly affected by the fraud.

Interviewing the suspects

Forensic auditor should interview only if the client gives mandate in the engagement letter. The basic difference between interview and interrogation is: interview is typically a less formal and the main objective is to elicit information; interrogation is formal and designed to get a suspect to confess.

Reporting

A report is required so that it can be presented to a client about the fraud identified. The report should include the brief scope of the work, findings of the investigation, a summary off the evidence, an explanation of how the fraud was perpetrated, who are the perpetrators and how long this has been going on and suggestions on how internal controls can be improved to prevent frauds in the future.

CASE STUDY-1

PQR Ltd is a multinational company with its headquarters in India. The company has been under scrutiny for its financial dealings with its subsidiary in a tax haven. Income Tax Department wants your firm to conduct a forensic audit to investigate whether PQR Ltd had siphoned off funds to its offshore entity to evade taxes. Elaborate the various steps that will be taken by your firm based on the concepts discussed in the above lesson.

Solution:

Siphoning off funds refers to the illegal practice of transferring funds from a company for personal gain or to hide illegal activities. There are several ways in which a company can siphon off funds, including:

Over-invoicing: A company may inflate the cost of goods or services purchased to receive a higher amount of money from the purchaser. The excess amount paid is then siphoned off for personal gain.

Under-invoicing: A company may undervalue goods or services sold to reduce the amount of tax payable. The difference between the actual value and the undervalued amount is then siphoned off.

Ghost employees: A company may create fake employees and pay them a salary, but in reality, the money is siphoned off by the company's management.

Round-tripping: A company may create fictitious transactions with a third party to show an increase in revenue. The third party then returns the money, and the company's management siphons off the amount.

Transfer pricing: A company may manipulate prices when transferring goods or services between its subsidiaries to reduce tax payable. The difference in prices is then siphoned off.

Misappropriation of funds: A company's management may directly take money from the company's accounts for personal use, without any legitimate reason or business purpose.

Offshore entities: A company may transfer funds to an offshore entity to evade taxes or hide illegal activities. The money is then siphoned off by the company's management.

These are some of the various ways a company can siphon off funds. It is important for companies to maintain transparency and ethical standards in their financial dealings to prevent such practices and avoid legal consequences. A forensic audit can help detect such fraudulent activities and bring perpetrators to justice.

The forensic audit revealed that PQR Ltd had indeed siphoned off funds to its subsidiary in the tax haven through a series of fraudulent transactions. The audit also found evidence of falsified invoices and inflated expenses to cover up the siphoning of funds.

The forensic audit report was presented as evidence in a court case filed by the Income Tax Department against PQR Ltd for tax evasion. The report was considered to be admissible evidence under the Indian Evidence Act, 1872.

The court found PQR Ltd guilty of tax evasion and ordered them to pay a substantial fine. The forensic audit report played a significant role in the court's decision as it provided concrete evidence of the fraudulent transactions and siphoning of funds by PQR Ltd.

CASE STUDY-2

A forensic audit was conducted to investigate allegations of financial irregularities and fraud in a public sector company. The forensic audit was carried out by a team of independent auditors appointed by the company's board of directors. The auditors examined the company's financial statements, accounting records, and other relevant documents to identify any discrepancies or irregularities.

During the forensic audit, the auditors uncovered evidence of fraudulent transactions and financial irregularities committed by certain employees of the company. The evidence included falsified invoices, manipulated accounting records, and unauthorized transactions. The auditors also found evidence that some of the employees had colluded with outside parties to carry out the fraud.

The Evidence Act of 1872 was crucial in this case, as it provided guidelines for the admissibility of evidence in legal proceedings. The forensic auditors were required to follow the procedures outlined in the Act to ensure that the evidence they gathered was admissible in court. The Act also provided guidelines for the cross-examination of witnesses and the presentation of evidence in court.

Based on the evidence gathered during the forensic audit, the company's board of directors took immediate action to terminate the employment of the employees involved in the fraud. The company also filed a criminal complaint with the police.

CASE STUDY-3

ABC Ltd. is a large manufacturing company that has been experiencing financial difficulties. The company has a number of subsidiaries and joint ventures, and its financial statements are complex and difficult to understand. The board of directors of ABC Ltd. suspect that there may be financial irregularities within the company, and they decide to conduct a forensic audit.

The board hires CS LLP as forensic accountants to conduct the forensic audit to detect the financial irregularities within the company. Elaborate the various steps that will be taken by CS LLP based on the concepts discussed in the above lesson without referring to the suggested solution below.

Solution:

CS LLP (Forensic auditors) will begin the forensic audit by examining the financial statements of ABC Ltd. and its subsidiaries and joint ventures with books of account and other records in the company to identify whether the allegation is true or not. They identified a number of unusual transactions and accounting entries that warranted further investigation.

Forensic auditors then conduct a series of interviews with key employees of ABC Ltd. and its subsidiaries and joint ventures. During these interviews, they uncovered evidence of fraud and financial irregularities, including falsified invoices, kickbacks, and unrecorded liabilities.

Based on the evidence gathered during the forensic audit and the forensic audit report submitted by the forensic auditors, the board of directors of ABC Ltd. decided to take legal action against the individuals responsible for the financial irregularities.

The board of directors after discussing with legal counsel filed a complaint with the police, and the case went to trial.

In the court, the evidence gathered during the forensic audit is presented to the Judge. The Judge relied on the Forensic Audit and Evidence Act, 1872 (the Act) to determine the admissibility of the evidence. The act provides guidelines for the admissibility of expert evidence, including forensic audit reports, in court.

The Judge determines that the evidence gathered during the forensic audit is admissible, and the individuals responsible for the financial irregularities are found guilty and sentenced to prison.

Thus Forensic audits can be an effective tool for investigating financial irregularities and fraud. The Indian Evidence Act, 1872 provides the legal framework for conducting forensic audits and using the evidence gathered in such audits in a court of law.

In the case study above, the forensic audit was able to uncover evidence of financial irregularities acceptable to the court of law, which led to successful prosecution and conviction of the individuals responsible.

LESSON ROUND-UP

- Sometimes the evidential fact is directly accessible to the fact-finder.
- A factual proposition (in Latin, factum probans) is evidence in the third sense only if it can serve as a premise for drawing an inference (directly or indirectly) to a matter that is material to the case (factum probandum).
- In summary, at least four possible conceptions of legal evidence are in currency: as an object of sensory evidence, as a fact, as an inferential premise and as that which counts as evidence in law. The sense in which the term “evidence” is being used is seldom made explicit in legal discourse although the intended meaning will often be clear from the context.

- In law, a question of law, also known as a point of law, is a question that must be answered by applying relevant legal principles to interpretation of the law.
- In law, a question of fact, also known as a point of fact, is a question that must be answered by reference to facts and evidence as well as inferences arising from those facts. Such a question is distinct from a question of law, which must be answered by applying relevant legal principles. The answer to a question of fact (a "finding of fact") usually depends on particular circumstances or factual situations.
- The law does not allow evidence to be adduced to prove facts that are immaterial or that are not in issue. "Relevance" is often used in the broader sense that encompasses the concepts under discussion.
- Thus for an evidence to have any value in the eyes of court of law and be relied upon on reaching the decision these few rules have to be kept in mind:
    1. Relevancy
    2. Admissibility
    3. Weight
- There are Two types of relevancy, which includes:
    1. Logical Relevancy and
    2. Legal Relevancy
- Every case, whether civil or criminal, that comes before a court of law has a fact story behind it. Facts out of which cases arise keep happening in the ordinary course of life. This concept is governed by the rules and regulations mentioned under Indian Evidence Act, 1872, Section 17-23.
- Oral evidence, as defined under Section 3 of the Evidence Act, means statements which the Court permits or requires to be made before it by witnesses in relation to matter of fact under inquiry.
- Under Section 3 of the Evidence Act, all documents including electronic records produced for the inspection of the Court together constitutes to be documentary evidence.
- In law, the production and presentation of evidence depends first on establishing on whom the burden of proof lays. Admissible evidence is that which a court receives and considers for the purposes of deciding a particular case.
- Two primary burden-of-proof considerations exist in law. The first is on whom the burden rests. In many, especially Western, courts, the burden of proof is placed on the prosecution. The second consideration is the degree of certitude proof must reach, depending on both the quantity and quality of evidence. These degrees are different for criminal and civil cases, the former requiring evidence beyond reasonable, the latter considering only which side has the preponderance of evidence, or whether the proposition is more likely true or false.
- The decision maker, often a jury, but sometimes a judge, decides whether the burden of proof has been fulfilled. After deciding who will carry the burden of proof, evidence is first gathered and then presented before the court.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation.)

Multiple Choice Questions 'MCQs'

1. Indian Evidence Act, 1872 came into force on?
    a) 15th March, 1872
    b) 1st September 1872
    c) 1st January 1873
    d) 1st June 1873
2. Facts under the Evidence Act means:
    a) Anything capable of being perceived by the senses and any mental condition of which any person is conscious
    b) Only any mental condition of which any person is conscious
    c) Anything capable of being perceived by the senses only
    d) Anything capable of being perceived by the senses only
3. Which Section of the Indian Evidence Act, 1872 deals only with civil matters?
    a) Section 27
    b) Section 133
    c) Section 23
    d) Section 53
4. Which one of the following sections of the Indian Evidence Act, 1872 provides that evidence may be given of facts in issue and relevant facts?
    a) Section 4
    b) Section 60
    c) Section 3
    d) Section 5
5. Electronics records produced before the court are:
    a) Ordinary evidence
    b) Technical evidence
    c) Oral evidence
    d) Documentary evidence
6. Which are the provisions under Indian Evidence Act, 1872 that deals with relevancy of opinion of experts?
    a) Sections 45 and 46
    b) Sections 81 and 82
    c) Sections 23 and 24
    d) Sections 49 and 50

7. Indian Evidence Act, 1872 applied to?
    a) Proceedings before Tribunals
    b) Proceedings before an arbitrator
    c) All judicial proceedings in or before any Court
    d) All the above
8. Evidence may be given in any suit or proceeding of the existence of non-existence of?
    a) Every fact in issue
    b) Such other facts as are hereinafter declared to be relevant
    c) Both A and B
    d) None of the above
9. A is tried for the murder of B by beating him with a club with the intention of causing his death. Which of the following facts are in issue at A's trial?
    a) A's beating B with the club
    b) A's causing B's death by such beating
    c) A's intention to cause B's death
    d) All of these
10. Facts which, though not in issue, are so connected with a fact in issue as to form part of the same transaction, are relevant, whether they occurred at the same time and place or at different times and places under Section?
    a) Under Section 5 of Indian Evidence Act, 1872
    b) Under Section 6 of Indian Evidence Act, 1872
    c) Under Section 7 of Indian Evidence Act, 1872
    d) Under Section 8 of Indian Evidence Act, 1872

Answers MCQ

1). b **2)**. a **3).** c **4).** d **5).** d **6).** a **7).** c **8).** c **9).** d **10).** b

Questions for Practice

1. What do you mean by Question of Fact and Question of Law?
2. What are the different types of evidences that are suitable in law useful for Forensic audit?
3. Discuss about the relevancy of Evidence.
4. What is meant by Admission of Evidence? Discuss in detail the provisions of Evidence Act, 1872.
5. What is meant by Positive Evidence and Negative Evidence?
6. Discuss the Direct and Circumstantial Methods of Proving a Case.

REFERENCES

1. Indian Evidence Act, 1872
2. Sir J.F. Stephen, Digest of the Law of Evidence

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

Cyber Forensics

Lesson 14

KEY CONCEPTS

■ Crime ■ Cyber Crime ■ Data Attack ■ Masquerading ■ Spear Phishing ■ Whaling ■ Vishing ■ Spamming ■ Smishing ■ Salami Attack ■ Web Jacking ■ Digital Forensics ■ Data Extraction ■ Ethical Hacking

Learning Objectives

To understand:

- The concept of cybercrime
- The classification of cybercrime
- Types of cybercrime such as Email spoofing, Hacking, Data Diddling etc.
- International guidance to cyber forensic laws
- The concept of digital forensics cyber laws
- What is Data Extraction
- The Concept of digital forensics and cyber crime
- What is Ethical Hacking?
- What is Digital Incident Response and the steps involved in it?

Lesson Outline

- Background to Cybercrime
- Meaning of Cyber Crime
- Types of Cyber Crime
- International Guidance to Cyber Forensics Laws
- Digital Forensics and Cyber Laws
- Data Extraction
- Digital Forensics and Cyber Crime
- Ethical Hacking
- Digital incidence response
- Case laws: Indian and International
- Lesson Round-Up
- Test Yourself
- List of Further Readings

BACKGROUND TO CYBERCRIME

It is a matter of pride that India has the second largest internet connection in the world. While having greater connectivity promises large-scale progress, it also leaves the citizens of our country exposed to new online vulnerabilities.

Cybercrime refers to criminal activities that are carried out using the internet or other forms of digital communication technology. Cybercriminals use these technologies to commit a wide range of criminal activities, including hacking, identity theft, phishing, cyber bullying, and online scams.

The development of digital technologies has led to the growth of the internet, social media, and other digital platforms that have become essential components of modern life. Criminals have found new ways to exploit vulnerabilities in these technologies.

The rise of the internet and digital communication technologies has led to a corresponding increase in cybercrime, which has become a major concern for Governments, Businesses, Corporates and Individuals around the world. They may target individuals, businesses, or even Governments to gain access to sensitive information, financial data, or intellectual property.

The consequences of cybercrime can be severe and wide-ranging. Victims may suffer financial losses, damage to their reputation, or even physical harm. Governments and businesses may also be affected, with cyber-attacks leading to the loss of confidential information, disruption of critical services, and other serious consequences.

The proliferation of digital technologies has created new opportunities for criminals to carry out their activities. For example, hackers can use the internet to gain unauthorized access to computer systems and steal sensitive information.

Phishing scams can be used to trick people into providing personal or financial information, while online scams can be used to defraud people of their money. Cyberbullying is also a growing problem, with individuals using digital technologies to harass, intimidate, or threaten others.

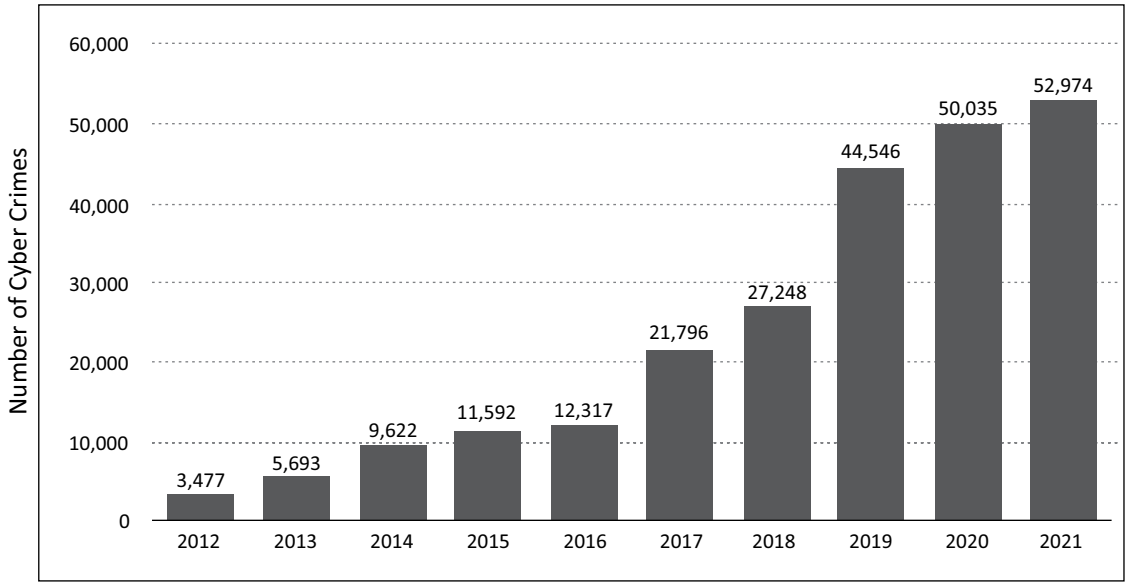
The rapid growth of the internet and digital communication technologies has also made it difficult to track and prosecute cybercriminals. Many cybercriminals operate across national borders, making it difficult for law enforcement agencies to coordinate and investigate crimes. Additionally, the nature of digital communication technologies makes it easy for cybercriminals to conceal their identities and location, further complicating law enforcement efforts.

As a result, there is a growing need for greater collaboration and cooperation between Governments, law enforcement agencies, and the private sector to combat cybercrime.

This includes the development of new technologies and strategies for preventing and detecting and responding to cybercrime by Governments and organisations, as well as increased investment in law enforcement and intelligence capabilities. It also involves greater public awareness and education about the risks and dangers of cybercrime.

These can include cybersecurity protocols, data protection laws, and the establishment of specialized law enforcement agencies. Preventive steps that individuals and organizations can take to protect themselves from cyber threats. However, the constantly evolving nature of cybercrime means that these measures must continually be updated and improved to stay ahead of the latest threats.

Number of cybercrimes reported across India from 2012 to 2021



https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

India saw a significant jump in cybercrimes reported in 2021 from the previous year possibly due to Covid pandemic forcing most of the citizens to transact online. That year, over 52 thousand cybercrime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. A majority of these cases were registered under the Information Technology Act, 2000 with the motive to defraud, or sexually exploit victims.

Roles and Responsibilities of the Board of Directors and Company Secretaries

Covid -19 pandemic has forced most of the entities across the world to innovate by initiating work from home and shifting to digital space to ensure business continuity. This has created an opportunity for online fraudsters and cybercriminals to exploit the vulnerability in networks as employees work from home. Today, a company's board of directors has a role in promoting overall organisational cyber health.

Key roles and responsibilities of the Board of Directors include: Cybersecurity Risk Oversight, Allocating sufficient manpower and financial resources, Proritising the material cyber risks, formulating risk mitigation plans. Board members have to take responsibility for the breaches and failures of the company's cyber security systems.

The Company Secretary is responsible for supporting the board and the Governance process, providing advice and guidance to the board on Information Technology Act and the appropriate regulations, company's own cyber security policies and ensuring best practice in Cybersecurity risk oversight.

MEANING OF CYBERCRIME

What is Crime?

Crime is defined as "an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law that makes the offender liable to punishment by that law" (Webster Dictionary).

What is Cybercrime?

Cybercrime as per European Commission 2007 has been defined as "criminals acts committed using electronic communications networks and information systems or against such network or systems".

Cybercrime is "a crime of any illegal activity committed either on or with a computer and the internet to steal personal identity, gaining unauthorised access to computer systems, sell contraband online or stalk victims online or disrupt operations with malevolent programs".

Through the medium of internet fraudsters' gain valuable sensitive information of companies, firms, individuals, banks and so forth. It can also lead to intellectual property crimes like stealing new product launch plans, new product description and marketing plans, list of potential customers, selling illegal articles, pornography/child pornography etc.

It is done using methods such as Phishing, Spoofing, Spamming, Pharming and so forth. Phishing refers to "an attack using mail programs to deceive internet users into disclosing confidential information that can be then exploited for illegal purposes".

Cybercrimes lead to financial loss, reputational loss, legal consequences, sabotage and theft of IPR. Human being is the weakest link and hence any negligence of human beings enables criminals to commit cybercrimes. Cybercrimes are now committed using mobile phones, tablets, Personal Digital Assistants (PDA) which has connectivity to internet.

Cybercrimes can cross borders in fractions of a second and impact several people in different countries at the same time. Melissa virus triggered havoc across the countries.

Melissa virus- On March 26, 2009, Microsoft Word 97 and Microsoft Word 2000 propagated virus via e-mail attachments. Its widespread attack affected a variety of sites throughout the internet. In Melissa attack, the email attachment is a .DOT Word document that contained a piece of malicious micro code. If an infected document in Word 97 or Word 2000 is opened, the embedded micro code will infect the Normal.dot template and cause any documents referencing this template to be infected with this macro virus.

Melissa virus is not the only virus that propagates itself through email attachments. Other viruses such as I Love You Virus (year 2000) and My Doom (year 2004) also propagates itself through email attachments.

Traditional white collar crime and Cybercrime

Traditional white collar crimes include Bribery, Corruption, Embezzlement or theft Forgery, Money laundering, Financial statements fraud, Identity theft, Procurement and contract fraud, Siphoning of funds and so on.

In both crimes there is no bloodshed and are perpetrated against individuals, society, organisations and the governments. The main difference lies in the modus operandi since in the case of cybercrime physical presence at the venue of the crime is not required.

In both the crimes fraud trail is left as an evidence which can be only detected by trained forensic experts. Let us understand how a computer can be a target and also used as a tool for committing cybercrime.

Computer as a Target

The computer system/ information stored on the computer are the target of the crime. Hackers broke into the system of Citibank in USA on June 9th 2011 and accessed the data of its customers, gained access to the online banking platform and viewed customer account numbers, contact information.

There are other cybercrimes using computer as a target like virus/worm attacks, Distributed Denial of Service (DDoS), Pornography etc.

Computer as a tool

The computer system/ or information stored on the computer system constitutes an important tool for committing the crime. Computer fraud, forgery like counterfeit currency notes, mark sheets, stamp papers, degree certificates can be done using sophisticated computers, printers and scanners , distribution of child pornography etc.

Motive and Reasons for Cybercrimes

Greed, Power hunger, Publicity, Revenge, Adventure or thrill seeking, Destructive mindset, Desire to access forbidden information have been observed as the motive and reasons for all Cybercrimes in the world.

Classification of Cybercrimes

Against Individuals – E-mail spoofing and other online frauds, Phishing, Spear Phishing, Vishing, Smishing, Spamming, Cyber defamation, Cyberstalking, Computer sabotage, Password sniffing, Pornographic offences and transmitting virus. These crimes are directed against individuals for various reasons ranging from greed to personal dispute.

Against Organisation- Hacking, Password sniffing, Denial of Service attack under section 43 of Information Technology Act,2000, E-mail bombing, Salami Attack/ Salami technique, Trojan Horse, Data Diddling, Industrial espionage, Software privacy, Cyber terrorism by rogue actors against any organisation.

Against Society and Governments- Hacking, Forgery (printing of counterfeit currency, forging passports, sale of illegal articles, online gambling, fake Stamp papers (Telgi scam) Cyberterrorism, Webjacking are directed against the society at large.

Against Property – Intellectual property, Credit card frauds, Internet time theft. Property refers also to software, computer source codes. These types of crimes are generally targeted against the society.

Accordance to the Information Technology Act, 2000 a Cyber Crime can be defined as "an act or omission that is punishable under the Information Technology Act, 2000". This however is not an exhaustive definition as the Indian Penal Code also covers certain cyber-crimes, such as email spoofing and cyber defamation, sending threatening emails, etc.

Cyber offences under the Act are tabulated below:

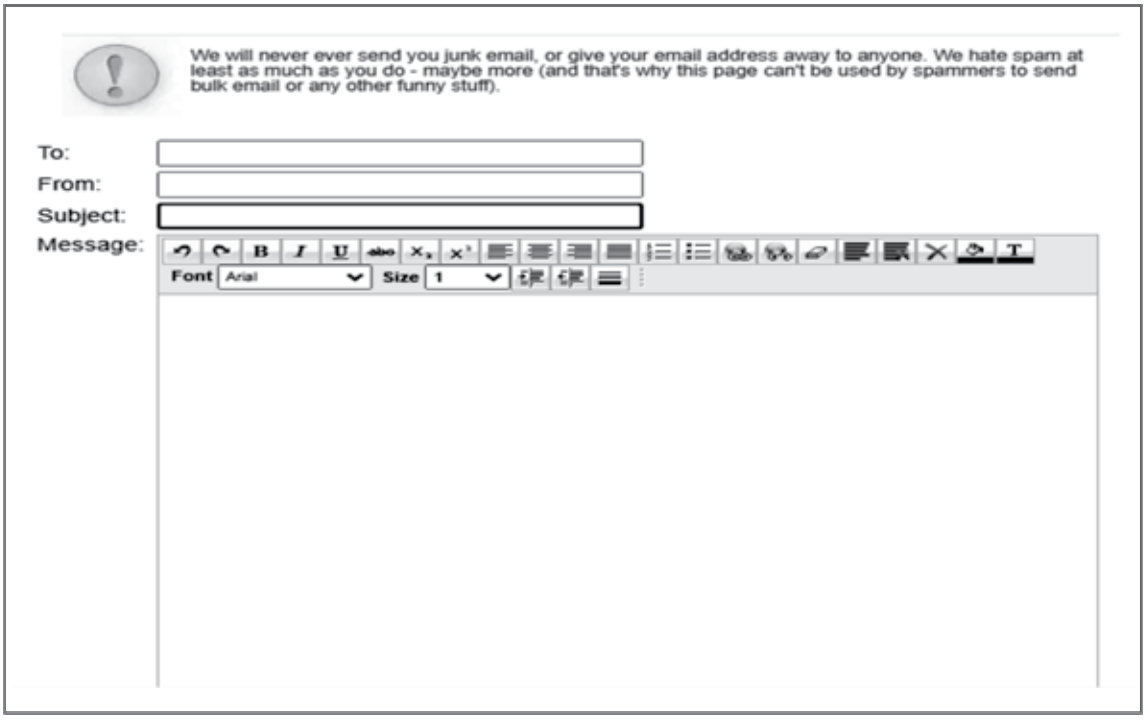
Section	***Offence***	***Description***
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.

Section	Offence	Description
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.
70	Securing access or attempting to secure access to a prote	The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.

TYPES OF CYBER CRIME

E-mail spoofing/ Phishing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. Free website are available to send fake emails. Anyone can fill any email address with the intention of deceiving the recipient of the email. When gullible receiver reads the mail/ he or she would think that the e-mail has been sent by legitimate sender based on the IP address indicating that the message has come from a trusted host. Phishing is an alternative of fishing, means to fish for information.



Source: http://deadfake.com/Send.aspx

The term Phishing was used in 1994-95 by hackers who were stealing American Online internet accounts by scamming passwords without the knowledge of AOL users (netizens). It is also an example of social engineering techniques used to deceive netizens. This was done using www.ao1.com instead of www.aol.com

Phishing is done to steal valuable personal and financial data like credit card details, passwords, PIN, social security numbers and bank account numbers by luring the victim to provide the account details and other personal information unwittingly.

E-mail spoofing is dealt under sections 416,417, 419, 463, 465 of Indian Penal Code.

Denial of Services/ Distributed Denial of Services

It is an attack to make a computer or network resource unavailable for the users either temporarily or permanently. DoS attackers target sites or services hosted by banks, airlines, hotel, credit card payment gateways etc. Cybercriminals prevent an internet site form functioning temporarily or even permanently.

Another Bot is a *spambot*, which gathers valid email addresses, so mailing lists can be created to send SPAM. Bots are particularly dangerous when they're deployed to large collections of computers, called *botnets*. Once a computer is infected, the bot can lay dormant until an attacker chooses to activate them. At this point, the

attacker has control of targeted computer (now called a *zombie*) and all the other computers in the botnet (also called a *zombie army*). The attacker can send a signal to have these computers distribute viruses, or send messages to a particular server in a coordinated attack called a *Distributed Denial of Service* attack.

It results in enormous financial and reputation loss as a result of such denial of service attack. It also leads to significant loss of time and money for the victim organisation as they have to rebuild from scratch.

There have been a number of instances of DoS attacks against India.

Distributed denial-of-service (DDoS) attacks are growing significantly across the world, and India ranks second as the largest source of Hypertext Transfer Protocol or HTTP-based DDoS attack traffic in July-September this year after China. China replaced the US as the main source of HTTP DDoS attack traffic in Q3.

Hacking

It was at Massachusetts Institute of Technology the word "Hack" was used in the late 1950's. In the 1960's the term seems to have migrated from the MIT to computer enthusiasts and in time, it has become an essential part of their lexicon. The meaning of hacking at that time was "fussing with machines".

Major reasons for hacking has been identified as: Greed, publicity, revenge, adventure and destructive mindset, strong desire to access forbidden and highly confidential information. Hackers write or use ready-made computer programs to attack the target computer and get enjoyment out of destruction. They exhort money from corporates threatening them that they will publish their stolen information. Government websites are always on hacker's target and attacks on the Government websites get wide publicity.

Every act committed towards breaking into computer and/or network is hacking and Hacking with intent or knowledge is an offence under section 66 of Information Technology Act, 2000 with a Fine of Rs.2 Lakhs and imprisonment for 3 years.

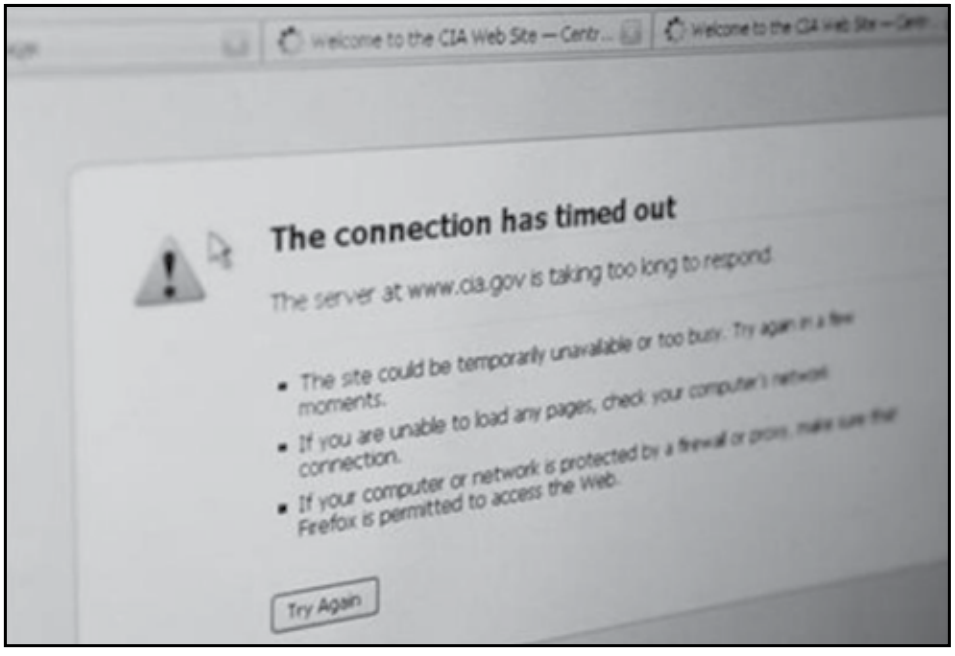
Real world examples of hacking

Nadya Suleman –Octomom's defaced website

Source: https://weeklyworldnews.com/headlines/6233/nadya-sulemans-website-hacked/

The public website of the Central Intelligence Agency went down on 15th June 2011 evening as the hacker group Lulz Security said it had launched an attack.

Source: https://www.reuters.com/article/us-cia-hackers-idUKTRE75E6JC20110616



The website of the U.S. Central Intelligence Agency (CIA) is unresponsive and unavailable after reports that the website had been attacked by internet hackers in Washington June 15, 2011. The Lulz Security group of hackers said in a Tweet that it had launched an attack on the public website of the U.S. Central Intelligence Agency. The site, www.cia.gov, was unavailable for a few minutes on evening, immediately after the group announced the attack via Twitter.

Data Attacks

According to 2022 Verizon Data Breach Investigation Report (DBIR) 5,212 breaches were analysed, 23,896 security incidents were reviewed. 82% breach involved the human element including social attacks, errors and misuse, 13% increase in Ransomware breaches which is more than in the last 5 years combined and 62% of incidents in the system intrusion pattern involved threat actors compromising partners. Over 50% of breaches involved use of either remote access or web applications. About 66% of breaches involved Phishing, stolen credentials and/or Ransomware.

The four key paths to data breaches are: Credentials, Phishing, Exploiting vulnerabilities and Botnets. No organisation is safe without a way to handle them.

Source: Verizon Data Breach Investigation Report, 2022

Data Diddling

It is one of the oldest form of computer crimes since the advent of electronic data processing. Data Diddling is changing of data either before or during entry into the computer system. Examples include forging or counterfeiting documents used for any data entry and replacing valid disks and tapes with tampered or modified disks and tapes. One of the earliest data diddling fraud was Equity Funding Corporation of America.

The NDMC Electricity Billing Fraud took place in 1996.The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and payment in the bank were exclusively left to a private contractor who was a computer professional.

He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

Section 66 [i] and 43(d) [ii] of the Information Technology Act, 2000 covers the offence of Data Diddling.

Masquerading

When a perpetrator pretends to be someone he is actually not by creating fake email ids, or uses someone else's user ID and password.

How is it done?

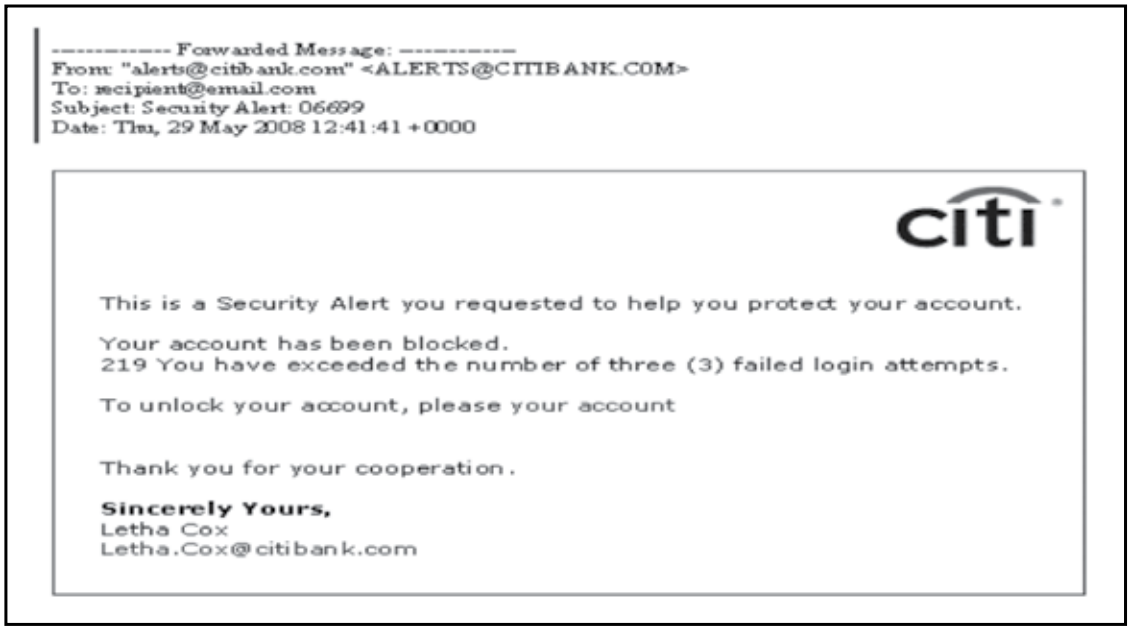
Cybercriminals browse the Facebook profiles and identify those posting profile pictures in police uniform and download profile picture and other photos. They also download the contact names of friends. They create fake account in the same name by using the downloaded photos from original social media account. They then send friend request to contact list and asks for money later. Fraudsters want money to be transferred to them through Google Pay, Paytm, PhonePe etc.

A fake Facebook account was created in the name of Raman (name changed), a sub-inspector of a rural police station, and messages were sent from it to his multiple Facebook friends, requesting money. One of the friends, without crosschecking, sent Rs 7,000 to the account mentioned in the message. There are many such instances of impersonating police officers across India for financial gain.

Spear Phishing

Any highly targeted e-mail attack that a scammer sends only to people within a small group. E-mail sent by the scammer appears genuine to all employees or members within the company or a Government department. Phishing scams are designed to steal information from individuals, Spear Phishing aims to gain access to an organisation's entire computer system. E-mail message might appear to be genuine, but if the recipient responds to it, he or she might put himself or herself and the employer at huge risk.

In Spear Phishing, targets are carefully chosen, and emails are carefully crafted with the specific target in mind. Few examples are given below:



---------- Forwarded Message: ----------
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000

citi

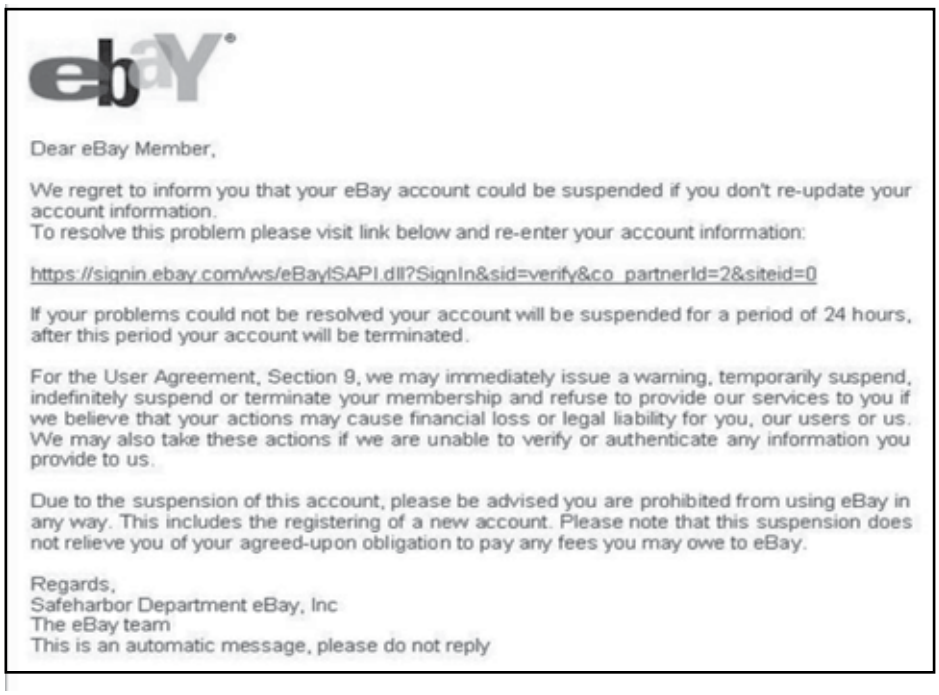
This is a Security Alert you requested to help you protect your account.

Your account has been blocked.
219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please your account

Thank you for your cooperation.

Sincerely Yours,
Letha Cox
Letha.Cox@citibank.com



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Whaling

This form of Spear Phishing targets top management C- Suites executives with the help of information obtained through Spear Phishing by installing malware for keylogging or other backdoor access mechanisms. E-mail is sent in the Whaling scam showing a sense of falsified urgency to transfer funds urgently and is meant to be tailored for executives as per example below:

FW: Urgent: Wire Transfer

LS Liam Sparks 10:34 PM
to Kaitlyn Taylor <kaitlyn.taylor@abcbank.com>

Hi Kaitlyn,

The attached invoice is still awaiting payment. The deadline is tomorrow and I am in an important meeting. Can you please wire over the funds as soon as you can?

Regards,

Liam
Manager, XYZ Supplies
t: +44 0184 667 7496

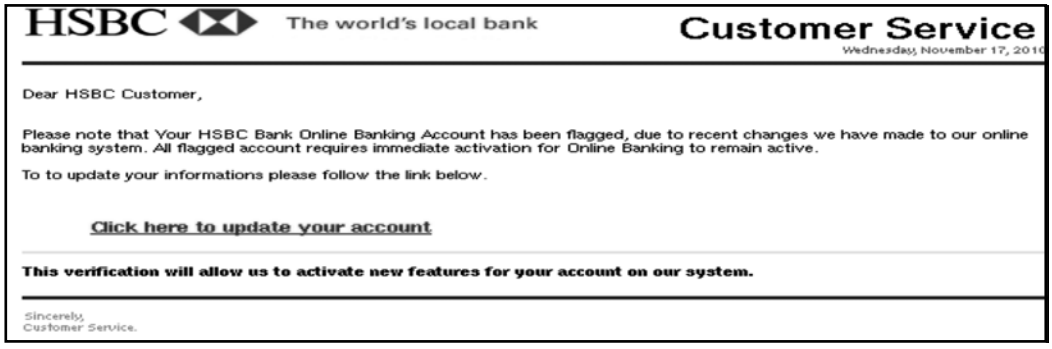
XYZ SUPPLIES

invoice_BAT_896352.pdf
486 kilobytes

Download Save to Onedrive

Vishing

The term is a combination of V-voice and Phishing and is usually used to steal credit card numbers or related data used in ID theft from individuals. Using a spoofed phone number and caller ID, the cybercriminal pretends to be calling on behalf of the victim's bank. The caller says that there has been unusual activity on the victim's account and asks the victim to confirm their bank account details, including their mailing address, for updating proof of identification (KYC) by sending a link. This information is then used by the cybercriminal to commit online banking fraud.


HSBC The world's local bank

Customer Service

Wednesday, November 17, 2010

Dear HSBC Customer,

Please note that Your HSBC Bank Online Banking Account has been flagged, due to recent changes we have made to our online banking system. All flagged account requires immediate activation for Online Banking to remain active.

To to update your informations please follow the link below.

Click here to update your account

This verification will allow us to activate new features for your account on our system.

Sincerely,
Customer Service.

Many examples are: Scammers offering to help the account holders with bank KYC updating by asking them to download an app and also by sharing the OTP. They also ask the victim to share the debit card details and OTP by claiming that the call is from the Bank.

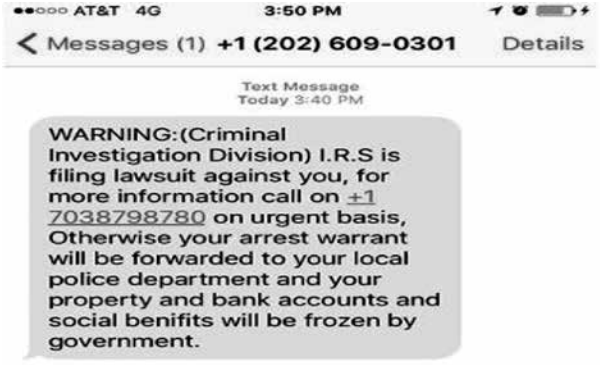
Spamming

Spam is abuse of electronic message systems by sending unsolicited bulk messages indiscriminately. Spamming is difficult to control since it is difficult to hold senders accountable for their mass mailings.

Botnet Email spam– though email is seen today as an older path for attack, spam botnets are some of the largest in size. They are primarily used for sending out spam messages, often including malware, in towering numbers from each bot. The Cutwail botnet founded in 2007, can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.

Smishing

The term is derived from SMS + PHISHING. The pretender hides the purpose and/or identity to get the personal information/ sensitive data about another individual. The criminal impersonates a legitimate entity such as an IT service/security admin, a bank, a government agency, an e-commerce site, a package delivery service, etc.



Cyber-defamation

It occurs when defamation takes place with the help of computers and internet. If someone publishes a defamatory matter about someone on a website or posts any defamatory message on any digital media.

India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

Section 499 of Chapter XXI of the Indian Penal Code defines Defamation:

Whoever by words either spoken or intended to be read or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm or knowing or having reason to believe that such imputation will harm the reputation of such person is said except in the case hereinafter expected to defame the person.

Cyber-stalking

It is the use of internet and/ electronic communication devices by an individual or groups of individuals to harass another individual or groups of individuals or an organisation by false accusations, monitoring, transmission of threats, damage to data or equipment and gathering information for harassment. Online stalkers aim to start the interaction with the targeted victim directly through internet. Email and Chatrooms are the most common form of medium used to connect with the victim.

Police (Delhi) arrest a man for cyberstalking woman: A 32-year-old man created a fake social media profile with obscene descriptions and photos of a woman and sent her obscene messages and photos after she ignored his messages on social media. A case was subsequently registered under Sections 67/67A (punishment for electronically transmitting obscenity in electronic form/sexual act in electronic form) of the Information Technology Act.

Computer sabotage/ vandalism

The use of internet to obstruct the normal functioning of a computer system or networks through worms, viruses or logic bomb. Cyber vandalism is a program which performs malicious function such as extracting users' password or other confidential data or even erasing hard disk.

Password sniffers & Key logger

Password sniffers are programs that monitor and record the user id and passwords. A key logger is a type of spyware that monitors and records user keystrokes including the ability to record mouse clicks. They allow cybercriminals to read anything a victim is typing into their keyboard, including private data like passwords, account numbers, and credit card numbers. They can be installed manually or automatically without user's knowledge, such as by inserting a flash drive into a USB slot or through a rootkit.

Transmitting virus

Computer virus is a software program that can infect legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves without the knowledge or permission of the users to potentially large numbers of programs on many machines.

- **Virus can be transmitted through the internet**

  Virus is intentionally uploaded on internet server or distributed through email. The internet server and hard disk gets infected with the virus. The virus then gets downloaded onto unsuspecting user if there are no anti-virus tool kit or outdated anti-virus tool kit is in the victim's computer.

- **Virus transmits through Stand-alone computer system**

  When Virus infected pen drive or disk is loaded to the stand alone computer either intentionally or unintentionally and hard disk gets infected.

- **Virus can be transmitted through local network**

  Virus is inserted in a legitimate program code and transmitted via data communication links to another node on the network. Virus then spreads itself to another nodes on the network.

Salami Attack

To commit a financial crime, an alteration is made so insignificant that it would go unnoticed. For example, if a bank employee inserts a program onto the bank server to deduct small amount of money make an unauthorised debit to bank account holders account and credit it to his fictitious bank account, he will be siphoning off a sizeable amount every month.

Theft of computer system and Internet time theft

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer. Internet time theft occurs when an unauthorised person uses the internet hours paid for by subscriber by hacking or gaining access by illegal means without the knowledge of the subscriber.

Intellectual Property Theft

Intellectual property rights means the ownership rights in intangible assets like software, source code, trade secrets, copyrights, and trade-marks. When the rights of an owner of an intellectual property right is deprived off either wholly or partially, it is called as intellectual property theft. There are many instances of piracy in the digital world since the advent of internet revolution. Online piracy or software piracy is the practice of downloading and distributing copyrighted works digitally without permission, such as music or feature films or software.

The Hyderabad Court in a land mark judgement convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software (Parthasarathy Pati case 16th March 2003).

Web Jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

Online Frauds

Online frauds are fraudulent activities such as an identity theft, financial frauds like online games or lotteries, free vacation.

Online job frauds

It involves misleading people who require a job by promising them a better job with higher pay while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

- **SIM swapping or SIM jacking**

  It is a fraudulent way of gaining access to someone's mobile number. It happens when a criminal convinces cellular provider to transfer victim's phone number to a different SIM (Subscriber Identity Module) card, usually one in their possession. If they succeed, victim will automatically at a disadvantage.

- **Cryptocurrency frauds**

  Cryptocurrency, such as bitcoin, is different from digital currency. It uses blockchain for verification and does not run through financial institutions, so it is harder to recover from theft.

- **Fake cryptocurrency exchanges**

  Scammers may lure investors in with promises of a great cryptocurrency exchange. But in reality, there is no exchange and the investor does not know it is fake until after they lose their deposit.

- **Ponzi schemes**

  To get fresh cryptocurrency investors, cryptocurrency scammers will lure new investors with bitcoin.

- **Bitcoin investment schemes**

  As part of the scheme, the so-called investment managers claim to have made millions investing in cryptocurrency and promise their victims that they will make money with investments. To get started, the scammers request an upfront fee. Then, instead of making money, the thieves simply steal the upfront fees. The scammers may also request personal identification information, claiming it's for transferring or depositing funds, and thus gain access to a person's cryptocurrency.

Conclusion

A broad overview about cybercrime and its various types have been explained in the above paragraphs. Various types of cybercrimes existing and new types of cybercrimes are happening every second in India and other parts of the globe. As a Corporate Governance Professionals we should be aware of the latest cyber scams and cyber frauds that are happening and necessary internal controls should be designed to protect the organisation and individuals from falling victim to it. As the technology is growing at mind-blowing pace post pandemic, many more new types of cybercrimes will emerge since fraudsters are always ahead in the conning game.

INTERNATIONAL GUIDANCE TO CYBER FORENSICS LAWS

Cyber forensic laws vary widely by country, and there is no one-size-fits-all approach to international guidance on this topic. However, there are a number of international agreements, conventions, and guidelines that countries can use as a basis for their own cyber forensic laws. Few of the conventions are given below.

Council of Europe Convention on Cybercrime:

As per Council of Europe Convention, Cybercrime are offences against and by means of computer systems. It has evolved into a significant threat to human rights, democracy and the rule of law as well as to international peace and stability, and it has major social and economic impact. In addition, any crime may involve evidence on a computer system needed in criminal investigations and proceedings.

Convention on Cybercrime (also known as the Budapest Convention)

The Budapest Convention 2001 is a criminal justice treaty that provides States with

i. the criminalisation of a list of attacks against and by means of computers;

ii. procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and

iii. International police and judicial cooperation on cybercrime and e-evidence.

The Budapest Convention provides a framework for countries to establish laws and procedures for investigating and prosecuting cybercrime and in international cooperation in investigating and prosecuting cybercrime

UN Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP), have jointly drafted and launched the *Practical Guide for Requesting Electronic Evidence Across Borders*.

Both, the 2018 and 2021 editions of the Practical Guide can be accessed by registered users of the CNA Directory. Access to the CNA Directory is reserved to central and competent national authorities and Permanent Missions to the United Nations.

DIGITAL FORENSICS AND CYBER LAWS

Digital forensics and cyber laws are two closely related fields that deal with investigating and prosecuting cybercrime.

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Cyber laws, on the other hand, are a set of regulations that govern online activities, including the use of the internet, computers, and other electronic devices. These laws are designed to protect individuals, businesses, and Governments from cybercrime and other illegal activities. Cyber laws cover a wide range of topics, including data privacy, intellectual property, and online harassment. In India, Information Technology Act, 2000, Indian Penal Code are the major legislations covering Cyberlaws.

Meaning of Digital Forensics as per International Criminal Police Organization (Interpol)

Digital forensics is “a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically”.

Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations. Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.

The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

DATA EXTRACTION

Data extraction is the process of collecting or retrieving dissimilar types of data from a variety of sources such as websites, databases and documents many of which may be poorly organised or completely unstructured.

With the help of Data extraction it is possible to clean, consolidate, process, and refine the data so that it can be stored in a centralised location in order to be transformed. These storage locations may be either on-site, cloud-based, or a hybrid of the two. Data extraction is the first step in both Extract, Transform, Load (ETL) and Extract, Load, Transform processes (ELT).

Data is extracted from a variety of sources and/or systems. The extraction locates and identifies relevant data and prepares it for processing or for transformation. Extraction allows many different types of data to be combined and finally mined for business intelligence or fraud detection.

Once the data has been successfully extracted it is now ready to be refined. In the transformation phase, data is sorted, organised, and cleaned. Duplicate entries will be deleted, missing values will be removed and audit will be performed to ensure that data is reliable, consistent, and usable. The transformed high quality data is then delivered to the target location for storage and analysis.

The ETL process is used by companies and organizations in every industry for many purposes. For instance, Healthcare companies need to extract many types of data from a range of local and cloud- based sources to streamline processes and support compliance efforts. Data extraction makes it possible to consolidate and integrate data related to patient care, healthcare providers, and insurance companies.

Similarly, retailers may able to collect customer information through mobile apps, websites, and in-store transactions. But without a way to migrate and merge all data, its potential may be limited. To solve this, data extraction is a solution.

Many companies and organisations take advantage of data extraction tools to manage the extraction process from end-to-end. Using an ETL tool automates and simplifies the extraction process thereby precious resources can be deployed toward other priorities.

The first step in data extraction is to identify the kinds of data required for analysis. Different types of data that are extracted by any entity may include Customer Data to help businesses and organisations in understanding their customers. It can include their names, contact details, purchase histories, social media activity, and web searches etc.

Financial Data Metrics include revenue, purchase cost, operating margins, and competitor's prices. This type of data helps companies to track its performance, improve efficiencies, and for doing strategic plan.

Task or process performance data: It includes information pertaining to specific tasks or operations. A retail company may seek information on its shipping logistics, or a Health care provider may want to monitor post-surgical results or patient feedback.

Once an organisation decides on the type of information it wants to access and analyse, the next steps are

1) Finding out where it can be got; and
2) Deciding where it wants to store it.

In most cases, it means moving data from one application, program, or server into another. Migration might involve data from services such as SAP, Amazon Web Services, MySQL, SQL Server, JSON, SalesForce etc. These are few widely used applications. However, data from any program, application, or server can be migrated.

To make things easy, one may use following data extraction tools for professionals as well as beginners –

OutWitHub

OutWithub is one of the most popular web scraping tools available in the market. It usually segregates the web pages into different elements and then navigates from page to page to extract the relevant data from the website. This tool has an extension for Mozilla Firefox and Chrome which makes it easy to access and is mainly used to extract links, email ids, data tables, images, etc.

Web Scraper

This is a very simple and easy-to-use web scraping tool available in the industry. It has the unique ability to login to external pages and is mainly used by companies for document extraction, web data scraping, email id extraction, pricing extraction, contact detail extraction, image extraction, etc.

Spinn3r

This is a web service which is used to index the blogs around the world. It provides access to every blog that is published in real-time and is mainly used by organizations to get information from social media, forums, web blogs, reviews, comments, mainstream news monitoring, etc.

Fminer

This is another popular tool used by companies which mainly acts as a visual web scraping tool, web data extractor, and a macro recorder. It is mainly used for disparate web scraping, email id extraction, phone number extraction, image extraction, document extraction, etc.

ParseHub

This is one of the most well-known visual extraction tools in the market which can be used by anyone to extract data from the web. The tool is mainly used to extract images, email ids, documents, web data, contact info, phone numbers, pricing details, etc.

Octaparse

This is one of the most powerful web scraping tools which can grab all the open data from any website and also save the user the effort of copy-pasting the information or any kind of further coding. This is mainly used to extract IP addresses, disparate data, email addresses, phone numbers, web data, etc.

Table Capture

This tool is an extension to the Chrome browser which helps to capture the data from the website while navigating through the web pages without any hassles. It easily scrapes the data from an HTML table of any website copies it to a clip board and converts it into any of the data formats such as Google spreadsheets, CSV, or Excel.

Scrapy

This is an open source code development framework which performs data extraction with Python. This tool allows developers to program crawlers to extract and track information for one or many websites at once.

Tabula

This is a desktop application for Mac OSX, Windows, and Linux, which helps companies and individuals to convert PDF files into an Excel or CSV file which can be easily edited. This is one of the most used extraction tools in data journalism.

Dexi.io

This web scraping tool doesn't need any kind of download and is a browser-based tool. This tool allows you to set up crawlers and fetch web data in real-time and also allows you to save the gathered information directly in the Google Drive or export it through CSV or JSON. One unique feature of this tool is that the data can be extracted anonymously using different proxy servers.

Impact of Cloud computing and IoT on Data Extraction

The advent of cloud computing has now a major impact in the manner companies and organisations manage and store their data. In addition to changes in data security, storage, and processing, the cloud computing has made now the ETL process more efficient and adaptable. Companies are able to access data from anywhere in the globe and process it in real-time, without having to maintain their own servers or investing in data infrastructure. Through the use of hybrid and cloud-based data options, more companies are beginning to move data away from legacy on-site systems.

Internet of Things (IoT) is also transforming the data landscape. In addition to mobile phones, tablets, and computers, data is now being generated by wearables such as FitBit, automobiles, household appliances, and even medical devices. The result is an ever-increasing amount of data can be used to drive a company's competitive edge, once the data has been extracted and transformed.

Practical Case Study

Domino's Pizza – Data Extraction

We all know that Domino's is the largest pizza company in the world. The main reason is its ability to receive orders from its consumers through a wide range of technologies, like smart phones, smart watches and even social media. All these channels generate an enormous amounts of data, which with help of information technology, the company integrates to produce insights into its global operations and customers' preferences.

To consolidate all of these data sources, Domino's uses a data management platform to manage its data from extraction to integration. Running on Domino's own cloud-based servers, this system captures and collects data from point of sales (POS) systems, 26 supply chain centres, and through various channels as different as text messages. Domino's data management platform then cleans, enriches and stores data so that it can be easily accessed and used by multiple teams and the product is delivered to the right customer and at the right time.

DIGITAL FORENSICS AND CYBER CRIME

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Cybercrime is "a crime of any illegal activity committed either on or with a computer and the internet to steal

personal identity, gaining unauthorised access to computer systems, sell contraband online or stalk victims online or disrupt operations with malevolent programs".

Digital Evidence

In order to solve a cybercrime alleged to have been committed appropriate digital evidence have to be identified and collected, analysed and evaluated as to the suitability in the court of law and report have to be prepared by the digital forensic expert and submitted to those who have appointed him.

There are many other storage media and technical devices that may process and store digital evidence. Examples of these devices include media cards (ie. secure digital, SIM card, flash, memory sticks), thumb drives, optical media (ie. CD, DVD, and Blu-ray), digital cameras, MP3 players, iPods, servers, surveillance systems, gaming stations (ie. Xbox, PlayStation, Wii), and GPS devices.

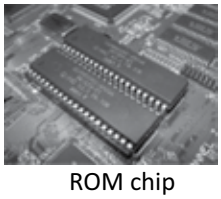
Each of these devices is capable of holding significant amount of data that could help to crack case. And each is handled in a separate way. Seizure of these items should be performed with special care. Always consider working with an experienced digital evidence analyst to collect these items.

Every sequence of events within a single computer might cause interactions with files and file systems in which they reside, other process and the programs they are executing. The files they produce and manage, log files and audit trails of various types. In a networked environment it extends to all networked devices. Evidence of an activity might be contained in a time stamp associated with a different program in a different computer as a digital forensics evidence.

Collecting volatile data requires specific technical skills. If the computer is still on, any intelligence that can be gained by examining the applications currently open is recorded. If information is stored solely in random access memory (RAM), is not recovered before switching down.

Embedded memories inside a computer comprises of

Read Only Memory (ROM) chip, Erasable Programmable Read Only Memory (EPROM) chip, Programmable Read Only Memory chip (PROM) and Electrify Erasable Programmable Read Only Memory (EEPROM) chip.


ROM chip


EPROM chip

PROM chip


EEPROM chip

Precautions to be adopted by Digital Forensics Expert

1. Take image of computer media using a write-blocking tool to ensure there is no data added or modification done to the suspected device. The process of creating an exact duplicate of the original evidentiary media is called imaging. Using hard drive duplicator or software, the entire hard disk drive is completely duplicated. The original disk drive is then securely stored to prevent tampering.

2. Establish and maintain Chain of Custody: Chain of custody means the chronological documentation, trail that indicates the seizure, custody of digital evidence, control, transfer, analysis and disposition of evidence, physical or electronic. Digital evidence by its very nature is invisible to the human eyes and hence evidence must be developed using sophisticated tools.

   The chain of custody requires that from the moment the evidence is collected, every transfer of evidence between persons should be documented to prove that nobody else could have accessed to that evidence. If the chain of custody is broken, the defendant can ask the court to declare the evidence as admissible.

3. Document everything.
4. Use only the tools and methods that have been tested and evaluated to validate the reliability of digital evidence**.**
5. Most valuable information that can be obtained in the course of digital forensic examination will come from interviewing the users, witnesses and the suspects. It can yield valuable information about the system configuration, applications, encryption keys and methodology to access encrypted files and network servers.
6. Without legal authority and unless the owner of the digital evidence has given consent to have the media examined, special care must be taken not to seize, copy and examine the data.
7. Due to the growing use of cryptographic storage, it may be that the only copy of the keys to decrypt the storage is in computer's memory. If the computer is switched off it will cause that information to be lost.

Digital Analysis

A digital investigation may involve many formats of digital data and therefore there are several types of analysis like Media analysis, media management analysis, file system analysis, Networking analysis, image analysis done by digital forensic experts.

Reporting

Once the digital analysis is completed based on the evidence gathered, interviews a report is prepared. After extracting and analysing the evidence the results may need to be presented before law enforcement officials, technical experts, legal experts and corporate management. Depending upon the nature of the incident or crime, it may become mandatory to present the findings in a court of law.

Most forensic reports, follow the general guideline below for a table of contents:

1. Brief summary of information
2. Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
3. Repository #1 (For example A's work computer)
   a. Summary of evidence found on Employee A's work computer
   b. Analysis of relevant portions of Employee A's work computer
      i. Email history
      ii. Internet search history
      Iii. USB registry analysis
      iv. Etc.

c. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)

4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the reports.

Source: https://www.thomsonreuters.com/en-us/posts/legal/understanding-digital-forensics-report/

Testifying

This phase involves presentation and cross-examination of expert witnesses. It depends on the country and legal framework in which cybercrime is registered. Digital forensics evidence is normally introduced by expert witness. Experts have a much specialised knowledge, skill, experience, training or specialised education about specific things of import to the matter on hand. Anyone put up as an expert who has no specialised knowledge can be seriously challenged by competent experts and counsel of the defendants.

There are broadly three types of personnel involved in digital forensics.

Technicians who carry out the technical aspects of gathering evidence as they have sufficient technical skills to gather information from various digital devices, understand software, hardware and network configurations.

Policy makers must establish forensics policies that is up to date and must be familiar with computing and forensics.

Professionals acts as a bridge between the technician and policy makers. They must have extensive technical skill and good understanding of laws.

Mobile Forensics

Mobile forensics, a part of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets is done in mobile forensics. All individuals depend on mobile devices for sending data receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.

A company may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud. Businesses have been known to track employees' personal usage of business devices in order to uncover evidence of illegal activity. Law enforcement, may be able to take advantage of mobile forensics by using electronic discovery to gather evidence.

Botnet Forensics

Botnet forensics determines the scope of the breach and applies the methodology to find out the type of the infection. It is an investigation of the botnet attacks. The prime objective of botnet forensics is to measure the level of intrusions, investigate the intrusions, and provide information on how to recover from an intrusion so as to strengthen system security.

ETHICAL HACKING

Ethical hacking is the practice of using hacking techniques for the purpose of identifying security vulnerabilities in computer systems and networks. The goal of ethical hacking is to improve the security posture of an organization by identifying and mitigating vulnerabilities before they can be exploited by malicious actors.

Ethical hackers, also known as white hat hackers, use the same tools and techniques as malicious hackers, but with the permission of the target organization. They perform penetration testing, vulnerability assessments, and other security testing activities to identify weaknesses in the target system.

Ethical hacking is an important aspect of modern cybersecurity, as it allows organizations to proactively identify and address security weaknesses before they can be exploited by attackers. It also helps organizations meet regulatory requirements and maintain compliance with industry standards.

However, ethical hacking must be conducted in a responsible and ethical manner. Ethical hackers must obtain permission from the target organization before conducting any testing, and must adhere to a strict code of ethics to ensure that their activities do not cause harm or damage to the target system or data.

DIGITAL INCIDENT RESPONSE

What is an Incident?

An incident is defined as the act of violating an explicit or implied security policy. Computer security incident is any adverse event which compromises some aspect of the computer or network security.

Digital Incident Response (IR) is the process of identifying, investigating, and responding to security incidents in computer networks and systems. The goal of digital incident response is to minimize the damage caused by an incident, contain the incident, and prevent future incidents from occurring.

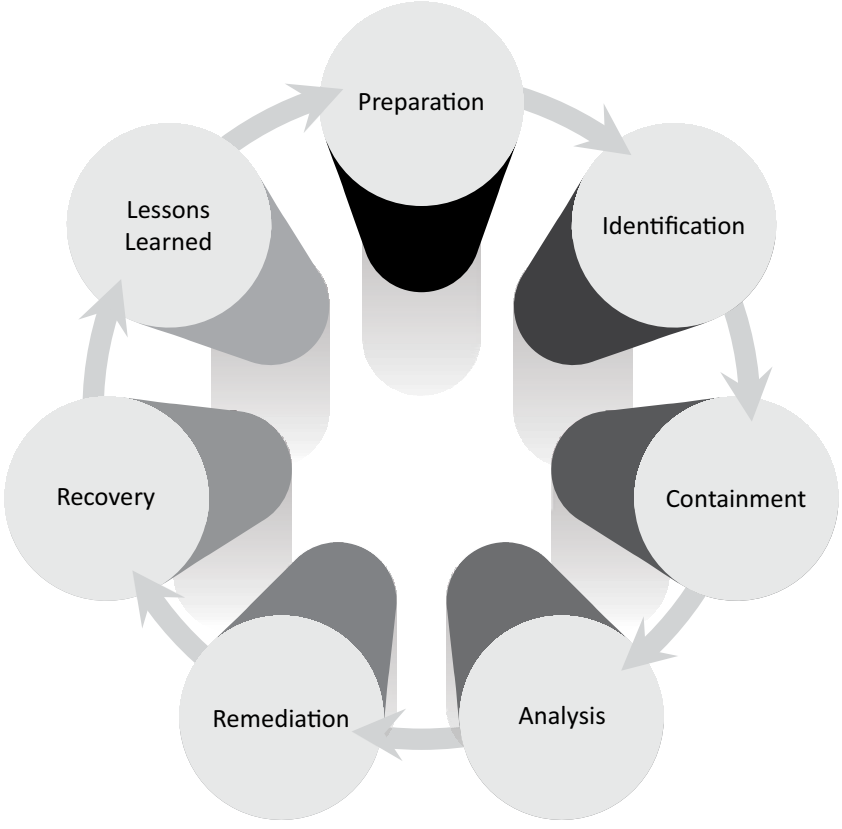
Due to frequent cyberattacks which compromise privacy of business data as well as personal privacy especially post pandemic incident response has become necessary. There have been many real incidents involving installation of malware and asking the victims to pay in cryptocurrency.

Recent case of cyberattack on AIIMS

Five servers of the All India Institute of Medical Sciences (AIIMS) were affected by the recent cyberattack in November 2022 and an estimated 1.3 terabytes of data was encrypted.

Based on the investigation it was found that the hackers had two Proton-mail addresses – “dog2398” and “mouse63209” these two addresses, ‘dog2398’ and ‘mouse63209’, were generated in the first week of November in Hong Kong. Another encrypted file was sent from Henan in China.

Digital Incidents Response Steps



The digital incident response process typically involves the following steps:

Preparation: This involves creating a plan for incident response, including identifying key personnel, establishing communication protocols, and developing a list of resources that can be used during an incident.

Identification: This involves detecting an incident by monitoring network activity and analyzing logs for signs of suspicious behavior. Incidents can also be identified through reports from users or other sources.

Containment: This involves isolating the affected systems and limiting the damage caused by the incident. This may involve shutting down systems, disconnecting them from the network, or blocking access to certain resources.

Analysis: This involves investigating the incident to determine the cause, scope, and impact of the incident. This may involve forensic analysis of systems and data to identify the source of the incident and gather evidence.

Remediation: This involves taking steps to address the vulnerabilities or weaknesses that allowed the incident to occur. This may involve patching systems, updating software, or implementing new security controls.

Recovery: This involves restoring systems and data to their normal state and verifying that the incident has been fully resolved.

Lessons learned: This involves reviewing the incident response process and identifying areas for improvement. This may involve updating incident response plans, improving monitoring and detection capabilities, or providing additional training to staff.

Digital incident response is a critical component of modern cybersecurity, as it allows organizations to quickly and effectively respond to security incidents and minimize the impact of a security breach.

CASE LAWS: INDIAN AND INTERNATIONAL

In India, cybercrimes are covered by the Information Technology Act, 2000 ('the Act') and the Indian Penal Code, 1860. It is the Act, deals with issues related to cybercrimes and electronic commerce in India. In the year 2008, the Act was amended and outlined the definition and punishment of cybercrime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

Information Technology Act, 2000 ("the Act")

Object of the Act

It is the first cyber law to be approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Some landmark Cases

1. ***Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank (PNB), HO New Delhi & Others (2018)***

   In 2013, in one of the largest compensation awarded in legal adjudication of a cybercrime dispute, Maharashtra's IT secretary Rajesh Aggarwal had ordered PNB to pay Rs 45 lakh to the Complainant Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. A fraudster had transferred Rs. 80.10 lakh from Matharu's account in PNB, Pune after Matharu responded to a phishing email. Complainant was asked to share the liability since he responded to the phishing mail but the Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the Complainant.

Punjab National Bank has gone on appeal against the above judgement to Telecom Disputes Settlement and Appellate Tribunal.

2. Pune Citibank MphasiS Call Center Fraud

Some ex-employees of BPO arm of MPhasiS Ltd, MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cybercrime cases that raised concerns of many kinds including the role of Data Protection". The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

Information Technology Act, 2000 **("the Act")** *is versatile enough to accommodate the aspects of crime not covered by the Act but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in the Act.*

Under the Act the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs. 1 crore per victim for which the "Adjudication Process" can be invoked.

3. Cyber Attack on Cosmos Bank

In August 2018, the Pune branch of Cosmos bank was drained of Rs. 94 crores, in an extremely bold cyber-attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred. According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out. This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

4. Bomb Hoax Mail

In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

International Case Study

FTX Scam

FTX Trading Limited (FTX) was founded in 2019 by Sam Bankman- Fried (SBF) and Gary Wang is now a bankrupt company having filed on November 11, 2022 Chapter 11 bankruptcy proceedings in the US Bankruptcy Court for the District of Delaware, losing over US$ 8 Billion in client money.

FTX formerly operated cryptocurrency exchange and crypto hedge fund. FTX means Futures Exchange. SBF was arrested on multiple fraud charges in November 2022.

FTX had closed to US$9 billion liabilities compared to just US$900 million in liquid assets comprising in shares in stock-trading App Robinhood.

He is now accused of fraudulent transfer of billions of US dollars of FTX client money to prop up his hedge fund Alameda Research. He deceived investors about the true risks at the company and artificially inflated the price of FTT token to access funding from investors.

How did FTX unravel?

CoinDesk publishes a report that revealed Alameda Research – a sister company to FTX – had a balance sheet full of FTT, the cryptocurrency issued by FTX. Changpeng Zhao, the founder of Binance, said the cryptocurrency exchange would offload all of its remaining FTT tokens "due to recent revelations that have come to light." FTT prices dropped as investors began to withdraw. Binance agrees to acquire FTX. Binance pulls out of its agreement to take over FTX.

Reference

Internet web pages on FTX scandal

LESSON ROUND-UP

- Everyone is getting increasingly dependent on consistent access and accuracy of these communication channels. The internet users have increased significantly especially in the last 15 years. This clearly indicates that the impact of Information Technology is very profound.
- Both Society and the Technology are operating in a way so as to harmonize with the pace of each other's growth. With boon comes the bane and thus the World of ICT is no exception to this rule. Along with abundant opportunities that it has brought about, there are also some challenges.
- Broadly speaking, it has posed certain major concerns like privacy threat, over riding cultural impact, more reliance on technology, boycott of societal engagements, computer virus, malware, spam phishing and many more. One of the major challenges in this era of ICT is of an increasing number of cyber crimes taking place in the World today.
- Cyber-crimes are technology based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. They are organized and white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft, etc.
- Digital forensics, as a developing discipline, presents a number of opportunities for international standardisation.
- Generally when procedures are standardised, the associated costs are lower, training is simplified and consumers accept products and services more readily.
- Cybersecurity professionals understand the value of this information and respect the fact that it can be easily compromised if not properly handled and protected.
- A key component of the investigative process involves the assessment of potential evidence in a cyber-crime. In order to effectively investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases.
- Data extraction is the act or process of retrieving data out of (usually unstructured or poorly structured) data sources for further data processing or data storage (data migration).
- An ethical hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

Multiple Choice Questions (MCQs)

1. Computer forensics also be used in civil proceedings.
    A. Yes
    B. No
    C. Can be yes or no
    D. Cannot say
2. *Forensic Auditors* are supposed to maintain three types of records. Which answer is not a record?
    A. Chain of custody
    B. Documentation of the crime scene
    C. Searching the crime scene
    D. Document your actions
3. Deleted files is a common technique used in computer forensics is the recovery of deleted files.
    A. TRUE
    B. FALSE
    C. Can be true or false
    D. Cannot say
4. All of the following are main type of computer forensics except:-
    A. Moral Forensics
    B. E-mail Forensics
    C. Malware Forensics
    D. Database Forensics
5. The main goal of computer forensics is:-
    A. Collect & Preserve the Data
    B. Identify the Data
    C. Analyse the Data
    D. All of the above
6. State whether True or False: Data encryption is primarily used to ensure confidentiality.
    A. True
    B. False
    C. Cannot be interpreted
    D. None

7. In which category does the lack of access control policy fall?
    A. Threat
    B. Bug
    C. Attack
    D. Vulnerability
8. Which software is mainly used to help users detect viruses and avoid them?
    A. Antivirus
    B. Adware
    C. Malware
    D. None
9. Identify the malware which does not replicate or clone through an infection?
    A. Trojans
    B. Worms
    C. Rootkits
    D. Virus
10. Choose the features which violate cyber security.
    A. Exploit
    B. Attack
    C. Compliance
    D. None

Answer:

1) A **2)** C **3)** A **4)** A **5)** D **6)** A **7)** D **8)** A **9)** A **10)** B

Practice Question

Every day, millions of computer users share files online. Shared file may be music, film, games, or software. File-sharing can give people access to a wealth of information. Your friend downloads special software that connects his computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software downloaded by the friend is free and easily accessible.

You are required to submit a detailed report on various aspects of the case based on the concepts given in this study lesson and give appropriate recommendations to your friend.

Theoretical Questions

1. What do you mean by Cyber Crime and role of forensic auditor?
2. What are the various types of Cyber Crime?

3. Write a brief note International Guidance to Cyber Forensics Laws.
4. What do you mean Data Extraction? Discuss the concept with examples.
5. Discuss the Concept of Ethical Hacking.
6. Explain the term 'Digital Forensics" along with example.
7. What is Digital Evidence?
8. What are the precautions to be adopted by Digital Forensic Expert?
9. Explain the term 'Mobile Forensics'
10. What is Digital Incident Response? Briefly narrate the steps involved in Digital Incident Response.

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann
- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

Fraud Detecting Techniques

Lesson 15

KEY CONCEPTS

■ Fraud ■ Investigation ■ Detection ■ Know Your Customer (KYC) ■ Misconduct ■ Digital Evidence ■ Clustering ■ Decision Tree

Learning Objectives

To understand:

- The meaning of Fraud, Investigation and Detection
- Early warning indicators of Fraud such as Unusual Financial Activity, Poor Accounting, Unusual behavior, Unexplained Inventory, Employee Turnover, Weak or lack of Internal Controls, Complaints or Tip, Weaknesses in IT Security, Suspicious Emails or Messages
- The term 'Money Laundering'
- Techniques used for Fraud Detection in Money Laundering
- Fraud Detection using General Audit Techniques such as Analytical procedures, Inquiry, Observation, Re-performance, Sampling, Inspection etc.
- Statistical and Mathematical Techniques in Fraud Detection
- Technology based Fraud Detection Techniques
- Data Mining Techniques for Fraud Detection

Lesson Outline

BACKGROUND TO FRAUD DETECTING TECHNIQUES

"There is enough in this world for every man's need, but there is not enough for every man's greed" – Mahatma Gandhi.

One of the major reason for frauds across the globe that is perpetrated by individuals or by an organisation is greed.

Meaning of Fraud: Wrongful or criminal deception intended to result in financial or personal gain.

Meaning of Investigation: The action of investigating something or someone; formal or systematic examination or research.

Meaning of Detection: The action or process of identifying the presence of something concealed.

Fraud investigation is a critical tool for protecting individuals and organisations from financial losses and ensuring that those who engage in fraudulent behavior are held accountable for their actions.

Fraud detection is a critical component of risk management for individuals and organisations. By employing effective fraud detection strategies, individuals and organisations can minimise their exposure to financial losses and reputational damage caused by fraud, while also promoting greater trust and security in their interactions with others.

As per Association of Certified Fraud Examiners (ACFE), Detection is an essential step in fraud investigation because the speed with which fraud is detected can have a substantial impact on the magnitude of fraud.

Fraud can take many forms and can be perpetrated by individuals or groups with various motivations. Common types of fraud include identity theft, credit card fraud, insurance fraud, and investment scams, among others. Fraudsters may use various tactics, such as impersonation, phishing, hacking, or social engineering, to gain access to sensitive information or manipulate victims into providing financial resources.

The Association of Certified Fraud Examiner's 2022 Report to the Nations time and again demonstrates that 42% of Fraud is detected only by way of Tip and of this 55% of tip came from Employees, 18% from the customers, Anonymous 16%. Fraud losses were 2X higher at organisations without hotlines. 45% of cases detected by tip with training within a period of 12 months with hotlines.

What is fraud detection?

Fraud detection is the process of identifying and preventing fraudulent activity in various contexts, including financial transactions, online interactions, insurance claims, and more. It is an important tool for individuals and organizations to protect themselves against financial losses and reputational damage caused by fraud. It is a postmortem after the alleged fraud has happened and a reactive action.

As seen above fraud can take many forms and it can be perpetrated by individuals or groups with various motivations. Common types of fraud include identity theft, credit card fraud, insurance fraud, and investment scams, among others. Fraudsters may use various tactics, such as impersonation, phishing, hacking, or social engineering, to gain access to sensitive information or manipulate victims into providing financial resources.

To effectively detect and prevent fraud, individuals and organizations must employ a range of strategies and tools. These may include automated systems for monitoring financial transactions, implementing secure authentication protocols, conducting background checks on individuals or organizations, and maintaining robust cybersecurity practices.

Fraud detection also requires a deep understanding of human behavior and the ability to identify patterns or anomalies that may indicate fraudulent activity. This may involve analysing data and behavior over time, identifying changes in behavior or activity that deviate from normal patterns, and conducting investigations to determine the root cause of suspicious activity.

It should be noted that the information technology is growing at a rapid pace especially after the COVID-19 pandemic across the globe. Company Secretaries in Industry or in Practice or as a Forensic Auditor cannot be an expert in all emerging technologies. Hence, the fraud detection tools discussed in this study lesson are very dynamic. What is relevant today may become obsolete tomorrow. Further, it involves working along with Data Scientists, Computer Scientists, Artificial Intelligence Researchers, Blockchain Developers and so forth.

EARLY WARNING INDICATORS OF FRAUD

1. **Unusual Financial Activity**

   This may include unexplained transactions, changes in account balances, or unexpected cash flow patterns, unexplained losses, increased expenses and/or decreased revenues.

2. **Poor Accounting or inconsistent or Missing Documentation**

   If financial records are incomplete, missing, or do not match up with other records, any accounting or record-keeping irregularities, such as missing documents, unexplained balances, or unrecorded transactions this could be a red flag for fraud.

3. **Unusual behavior or Changes in behavior or lifestyle by Employees**

   This could include employees who suddenly start working unusual hours, show signs of financial stress, or exhibit other unusual behaviors. Keep an eye or understand from interviewing with key persons if they observed any sudden changes in behavior or lifestyle of employees or stakeholders. For example, if an employee suddenly starts buying expensive items, it could be a red flag.

As per ACFE 2022 report 85% of all fraudsters displayed at least one behavioral red flag: 39% (Living beyond means), 25% (Financial difficulties), and 20% (unusual close relationship with vendors), and 13% (unwillingness to share duties).

4. **Unexplained Inventory or Movable Assets Shortages**

   If inventory levels or movable assets are lower than expected or if there is a discrepancy between inventory levels, movable assets and its records, this could be a sign of fraud. Stealing of inventory happens in industry in trading and manufacturing of consumer goods like high value mobile phones, tablets, laptops etc.

5. **Employee Turnover**

   High employee turnover, particularly in key financial roles, could be a sign of fraudulent activity which needs to be carefully probed.

6. **Weak or lack of Internal Controls**

   If an organisation has weak internal controls, this could make it easier for fraud to occur. Be aware of any instances where there is a lack of internal controls or segregation of duties, which could make it easier for fraud to occur.

7. **Complaints or Tip**

   If employees, customers, or vendors report suspicious activity, this should be taken seriously and investigated since majority of frauds are detected based on Complaints or tip and not by an internal audit or external audit.

8. **Weaknesses in IT Security**

   Any weaknesses in IT security that could allow unauthorised access to sensitive data or transactions. Many entities in addition to financial audit also do audit of their systems and network with the help of Vulnerability assessment and Penetration testing (VAPT).

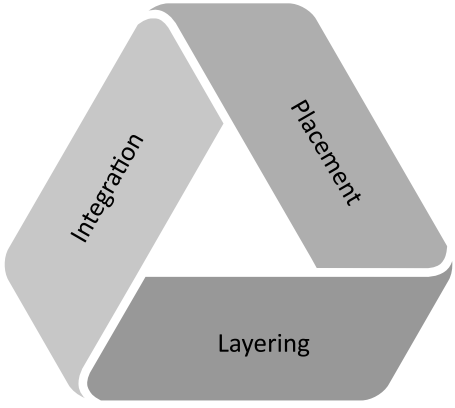
9. **Suspicious Emails or Messages**

   If employees receive emails or messages that appear to be from a legitimate company or organisation, but are asked to click on a link or provide additional information, it could be a phishing scam designed to steal entity's information.

   By monitoring these early warning indicators and implementing strong internal controls, organisations can help prevent fraud and minimize its impact if it does occur.

MONEY LAUNDERING AND ITS DETECTION

Money laundering starts with proceeds from a specific source. For a variety of reasons the launderer wants to hide the money trail. Money laundering takes place in three distinct stages: Placement, Layering and Integration. The money launderers including drug dealers, fraudsters, tax evaders and terrorists have many challenges when moving money through each of the stage.



Placement: The placement of funds of illegal proceeds into a financial institution is the first stage of money laundering and it is not so easy to do. The challenge is mainly due to dealers deal in hard currency. Placing the cash into a financial system undetected is difficult because the banks are required to file a report with the Government for all cash deposits in excess of threshold limit. For example in the United States and Canada any cash deposits in excess of $ 10,000 is automatically picked up by the reporting system.

According to the new rules, PAN and Aadhaar will be required for depositing cash more than the threshold limit in a bank or post office in any one financial year.

A bank (both private and nationalized bank) has to furnish a Cash Transaction Report (CTR) to the Financial Intelligence Unit (FIU) every month "incorporating all transactions over 10 lakh or its equivalent in foreign currency or a series of integrally connected transactions that add up to more than 10 lakh or its equivalent in foreign currency."

The FIU is empowered to get the CTRs under the Prevention of Money Laundering Act (PMLA). There have been CTRs where numerous small transactions were undertaken without mentioning the PAN and when these are inter-linked with the help of data mining tools a big picture of possible tax evasion or money laundering emerges.

To avoid their cash deposits from being reported, the launderers use a technique known as "smurfing". Smurfs known as "mules" are individuals recruited to open bank account and deposit cash in amount smaller than threshold limits prescribed in their countries. But moving millions of dollars or rupees can be a time consuming process and such suspicious movement of funds are also tracked by bank's software.

Hence, money launderer often purchase business that deal in cash like restaurants, bars, night clubs, malls, cinema theatre etc. and comingle their illegal proceeds with the funds of their business.

Layering

Once the proceeds of crime have been successfully injected into the financial system, the next stage is layering transactions by moving the proceeds through various banks or financial transactions. Law firms specializing in creating off-shore accounts can be used to set up shell companies, trusts or a foundation to purchase assets internationally.

In the case of transnational criminal matter, Mutual Legal Assistance Treaty (MLAT) has to be used, if both the prosecutor's country of origin and the subject's country of origin have entered into an MLAT. If there is no MLAT in place, letters rogatory (letters of request) are used to facilitate communication. Letters rogatory is slower and cumbersome than MLAT.

Due to the time delay in getting MLAT and LR, an astute money launderer could swiftly move funds through a number of foreign jurisdictions, effectively preventing law enforcement from tracing the money.

Money laundering is a complex process involving the concealment of the proceeds of illegal activities by disguising them as legitimate funds. Fraud detection techniques can be used to identify suspicious activities that may be indicative of money laundering.

Integration

The last stage of money laundering is moving the layered money into an account that appears to be for a legitimate purpose. Funds can be moved into clean bank account with explanations such as consulting fee, loan, dividend via wire transfer from an overseas shell company's bank account.

Techniques used for Fraud Detection in Money Laundering

Some of the common techniques used for fraud detection in money laundering include:

1. **Transaction Monitoring**

   Transaction monitoring involves the continuous surveillance of financial transactions to detect and flag suspicious activities. This involves the use of automated software programs to track transactions in real-time, analyse patterns, and identify anomalies or unusual behavior. Transaction monitoring is an automated process used to identify and analyse transactions for any unusual or suspicious patterns. The system analyses data such as the amount, frequency, and destination of transactions to identify any red flags.

2. **Customer Due Diligence (CDD)**

   CDD is a process of identifying and verifying the identity of customers, including their source of funds and the purpose of their transactions. This can help identify potential money launderers and high-risk customers.

3. **Know Your Customer (KYC)**

   KYC is similar to CDD but focuses on building a more detailed understanding of customers by gathering information about their financial behavior, transaction history, and risk profile. KYC is a mandatory process for financial institutions to identify and verify the identity of their customers. KYC helps to prevent fraud by ensuring that the customer is legitimate and not involved in any illegal activities.

4. **Enhanced Due Diligence (EDD)**

   EDD is a more intensive form of CDD and KYC, typically used for high-risk customers or those with complex transactions. This involves a deeper investigation of the customer's financial activity, including the source of funds, the purpose of transactions, and the nature of the relationship with the financial institution.

5. **Risk-Based Approach (RBA)**

   RBA involves assessing the level of risk posed by a customer, transaction, or business and applying appropriate measures to mitigate that risk. This can help financial institutions prioritise their efforts and resources in identifying potential money laundering activities.

6. **Artificial Intelligence (AI) and Machine Learning (ML)**

   AI and machine learning algorithms can be used to analyse large volumes of data, identify patterns, and detect suspicious activities in real-time. This can help financial institutions stay ahead of money launderers and adapt to changing fraud patterns.

7. **Suspicious Activity Reporting (SAR)**

   Financial institutions should monitor customer accounts for any suspicious activity, such as sudden large deposits, unusual transactions, or multiple transactions to the same destination. This can help to detect potential money laundering activities.

   SAR is a process of reporting suspicious transactions to relevant authorities, such as law enforcement or regulatory bodies. This can help to identify and investigate potential money laundering activities and prevent further criminal activity.

8. **Link Analysis**

   Link analysis is very effective for identifying the indirect link. When conducting a money laundering probe, link analysis is useful to track the placement, layering and integration of money as it moves around unexpected sources. It helps to uncover indirect relationships including those that are connected through

maze of subsidiaries. It can also help to detect a shell company. The forensic auditor could link between varieties of entities that commonly share an address.

How to detect shell companies using link analysis

It has been observed that most of the money laundering involves use of shell companies for doing money laundering. Detection of it involves examining the relationships between entities and identifying suspicious patterns.

- **Identify the Key Entities**: The first step is to identify the key entities that have to be analysed. These could be companies, individuals, or any other relevant entities.
- **Collect Data**: Collect data on the identified entities from various sources, including public records, corporate filings, social media, and other online sources.
- **Build a Chart**: Build a chart representing the relationships between the entities.
- **Analyze the Chart**: Use link analysis techniques to identify suspicious patterns in the chart. Look for entities that are linked to multiple other entities or that have unusual patterns of connections.
- **Look for Red Flags:** Look for red flags that may indicate the presence of a shell company, such as a company with no employees or physical location, a company with a history of frequent name changes or ownership changes, or a company that is linked to other suspicious entities.
- I**nvestigate further:** If auditor identifies a suspicious entity, investigate further to gather more information and verify the findings. He may need to conduct additional research or consult with experts in the field to determine whether the entity is a shell company.
- **Risk Assessment**: Financial institutions should conduct a risk assessment of their customers and transactions to identify high-risk customers and transactions. This helps to allocate resources and prioritize investigations on high-risk transactions.
- **Watch list Screening:** Watch list screening involves comparing customer names against government and international watch lists of known criminals, terrorists, and politically exposed persons (PEPs). This helps to identify high-risk customers and transactions and prevent money laundering activities.
- **Data Analytics:** Financial institutions can use data analytics to identify patterns and trends in customer transactions, enabling them to identify potential money laundering activities.

Overall, fraud detection techniques in money laundering require a combination of technological solutions, human expertise, and regulatory frameworks to be effective in detecting and preventing criminal activities.

MISCONDUCT

Asset misappropriation is a fraudulent conduct (or misconduct). Data analysis helps to detect frauds especially in bigger organisation with many employees, customers, vendors and due to a large amount of data, manual forensic audit is impractical. Inserting Ghost or fictitious employees in the payroll register are those who does not actually work for the entity. Detecting fraudulent payments and siphoning off funds can be detected with data analysis to cover ghost employees.

Tests that can help unravel fictitious employees are:

1. Check whether multiple employees are using the same bank account
2. Employee using multiple bank accounts
3. Multiple employees have same home address

4. Employees still on the payroll even after resignation/dismissal/ retirement date
5. Head count analysis department wise.

With the help of IDEA DATA analysis software etc., test for employees with the same address can be made as a process of fraud detection.

FRAUD DETECTION USING GENERAL AUDIT TECHNIQUES

Fraud detection is an important objective of any audit be it internal audit or statutory audit or a cost audit. General audit techniques can also be used and is very helpful to identify potential fraud risks and to gather evidence of fraudulent activities.

The responsibilities of the external auditor as they relate to fraud detection are clearly defined in International Standard on Auditing (ISA-240), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.

"The auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement"

Some of the general audit techniques that can be used by auditors to detect fraud include:

1. **Analytical procedures**

   This involves analysing financial data to identify trends or anomalies that may indicate fraud. For example, the auditor can compare financial ratios with industry benchmarks or prior periods to identify unusual changes in the company's financial performance.

2. **Inquiry**

   This involves asking questions of management and other employees to identify potential fraud risks and to gather information about the company's internal control systems. The auditor can ask about unusual transactions, discrepancies in records, or unusual behavior by employees.

3. **Observation**

   This involves physically observing the company's operations to identify potential fraud risks. For example, the auditor can observe how cash is collected and counted to identify any weaknesses in the company's movable assets handling procedures which are susceptible to fraud.

4. **Re-performance**

   This involves re-performing calculations or procedures performed by the client to ensure their accuracy. This can help the auditor identify errors or discrepancies that may indicate fraudulent activities.

5. **Sampling**

   This involves selecting a representative sample of transactions or data to test for accuracy and completeness. This can help the auditor identify unusual transactions or patterns of behavior that may indicate fraud.

6. **Inspection**

   This involves examining records and documents, such as invoices, receipts, contracts, and bank statements, to verify their accuracy and completeness. This can help the auditor identify fraudulent transactions or falsified documents.

   In addition to the above mentioned general audit techniques, auditors can also use specialised audit procedures to detect fraud, such as data analytics and forensic accounting techniques.

The key to effective fraud detection is to be vigilant, skeptical, and thorough in gathering and evaluating audit evidence.

STATISTICAL AND MATHEMATICAL TECHNIQUES IN FRAUD DETECTION

Statistical and mathematical techniques play a crucial role in fraud detection techniques, as they enable financial institutions to identify and analyze large volumes of data to detect potential fraud patterns.

Here are some commonly used statistical and mathematical techniques in fraud detection:

Benford's Law

Frank Benford in 1920's made an interesting observation while examining his logarithm book. He noticed that the first few pages of his logarithm book were more worn out than the other pages. His theory was scientists spend more time dealing with logs that begin with 1, 2 or 3 and with each succeeding first digit the time it was used was decreased.

This led to remarkable mathematical discovery. In a population of naturally occurring multi-digit numbers, the multi-digit numbers beginning with 1, 2 or 3 must appear more frequently than multi-digit numbers beginning with digits 4 to 9.Benford law cannot be applied for non-natural numbers like Employee ID numbers, telephone numbers which are designed systematically to convey information that restricts the natural nature of the number.

Benford's law provides that the distribution of the digit in multi-digit natural number is not random but it follows a pattern which can be predicted. The goal of a Benford's law is to identify fictitious numbers when creating false documentation or transactions to cover the tracks by fraudsters.

Benford's Law is a statistical tool used to detect potential fraud in financial statements or other numerical datasets. The law states that in many naturally occurring datasets, the leading digit is more likely to be a small number (e.g., 1, 2, or 3) than a large number (e.g., 8 or 9).

One application of Benford's Law is in detecting fraudulent journal entries or fraudulent financial transactions in the books of account.

Suppose a company's financial statements show that there were several large expenses recorded during a particular period. A forensic accountant or auditor could use Benford's Law to investigate whether the expenses were legitimate or if they were inflated or fraudulent.

To do this, they would first examine the leading digits of the journal entries and calculate the expected frequency of each digit according to Benford's Law. If the actual frequencies differ significantly from the expected frequencies, it could indicate that the numbers were manipulated or fabricated.

Example:

A company's financial statements it is suspected that there were few fictitious expenses recorded during the year, with the following amounts in INR:

22,500

10,750

8,650

14,200

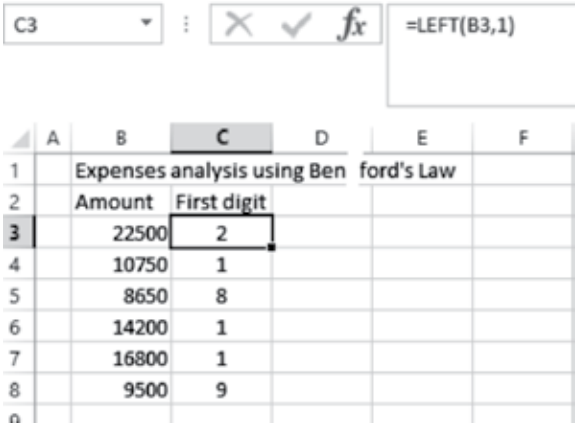
16,800

9,500

Using Benford's Law, forensic auditor would expect the following frequencies for the leading digit:

(1) 30.1%
(2) 17.6%
(3) 12.5%
(4) 9.7%
(5) 7.9%
(6) 6.7%
(7) 5.8%
(8) 5.1%
(9) 4.6%

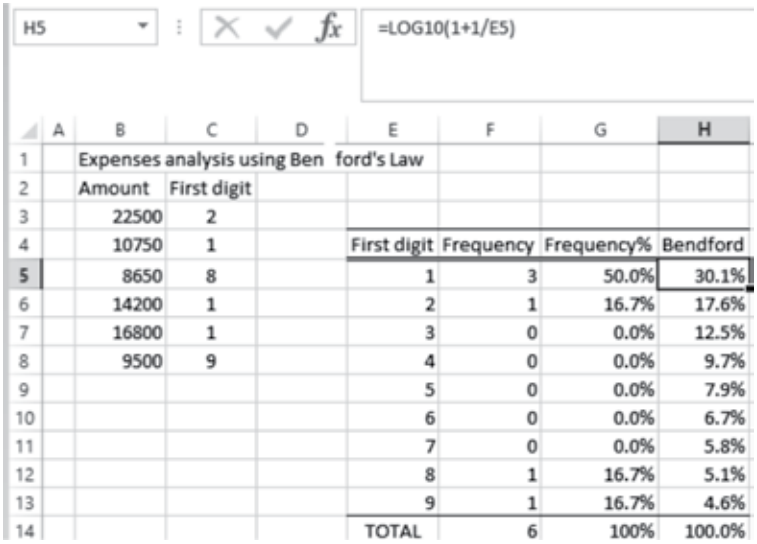
Extract the first digit from each number in column C using the LEFT function, and copied it down.



Let's make a table and look at the frequency of each digit.

Use the COUNTIF function to count how many times each digit (1 through 9) occurs in column C and let's check our numbers against Benford's law.

The Excel formula for Benford's Law is =LOG10(1+1/d), where **d** is the leading digit:



By calculating the actual frequencies for the first leading digit of the above journal entries, we get:

(1) 50%

(2) 16.7%

(3) 0%

(4) 0%

(5) 0%

(6) 0%

(7) 0%

(8) 16.7%

(9) 16.7%

In this example, the actual frequencies for the leading digit do not match the expected frequencies according to Benford's Law, which could indicate that the expenses were manipulated or fraudulent. Further investigation would be necessary to determine the cause of the discrepancy and whether fraudulent activity occurred.

Illustration:

There were 500 cheque payment vouchers in a month. Out of this at least 150 (30% of 500) vouchers must begin with 1. It means cheques can be for Rs.19, Rs.100, Rs.100, 000 and so on.

The actual payments are stratified or segmented for transactions beginning with each digit and these transactions are counted and summarised as below.

First digit	***No of transactions***
1	165
2	88
3	63
4	49
5	38
6	33
7	28
8	26
9	10
TOTAL	500

As the head of forensic audit team, you are required to guide your team as to how they should proceed to unearth the fraud using Benford Law.

Solution:

First digit	*No of transactions*	*Frequency%*	*Benford*	*Variance*	*Remarks*
1	165	33.0%	30.1%	2.9%	Error/ Fraud expected
2	88	17.6%	17.6%	0.0%	
3	63	12.6%	12.5%	0.1%	
4	49	9.8%	9.7%	0.1%	
5	38	7.6%	7.9%	-0.3%	
6	33	6.6%	6.7%	-0.1%	
7	28	5.6%	5.8%	-0.2%	
8	26	5.2%	5.1%	0.1%	
9	10	2.0%	4.6%	-2.6%	Error/ Fraud expected
TOTAL	500	100%	100.0%		

The forensic team should focus on all the transactions having huge variances since Error or Fraud is expected applying Benford's law. This will help to detect whether fraud or error has happened in the entity.

Regression Analysis

Regression analysis is a statistical technique that examines the relationship between two or more variables. In fraud detection, regression analysis can be used to identify relationships between variables, such as the correlation between high-risk customers and suspicious transactions.

Suppose an insurance company wants to detect fraudulent claims made by its customers. The company collects data on the claims made by its customers, including the type of claim, amount of the claim, and other relevant details. The data is then analysed using regression analysis to identify relationships between the variables and detect any unusual patterns.

In this case, the company can use regression analysis to model the relationship between the amount of the claim and other relevant variables, such as the type of claim, the location of the claim, and the history of the claimant.

By using multiple regression analysis, the company can identify suspicious claims that are outside the normal behavior of its customers.

For example, if a regression model indicates that claims of a certain type and location are usually of a specific range of amounts, and a claimant suddenly files a claim outside that range, it may indicate fraudulent activity.

Additionally, the regression model can be used to compare the characteristics of these suspicious claims with past fraud cases to determine if they are similar or not.

Cluster Analysis

Cluster analysis is a statistical technique that groups similar data points together.

Suppose a credit card company wants to detect fraudulent activities in its transactions. The company collects data on the transactions made by its customers, including the transaction amount, location, time, and other

relevant details. The data is then analyzed using cluster analysis to identify patterns and groups of transactions that are similar to each other.

In this case, the company can use cluster analysis to group transactions based on their characteristics, such as the location, time, and amount of the transaction. The analysis can help identify clusters of transactions that are outside the normal behavior of the customers, and hence may be indicative of fraud.

For instance, if a cluster of transactions is identified that occurred at unusual locations and times, with higher than average transaction amounts, it may indicate fraudulent activity.

Additionally, the cluster analysis can be used to compare the characteristics of these suspicious clusters with past fraud cases to determine if they are similar or not.

Real life example

During Covid-19 lockdown time when no one was allowed to fly out of India, one of the customer of a credit card company got a confirmation call from the bank alerting in the middle of the night stating that his credit card has been swiped in Thailand. Whether the customer is approving it or not?

Having known that it was a fraudulent transaction purported to be attempt, the card was blocked at the request of the customer and the transaction was declined. This call was based on the automated suspicion report to protect the interest of its customers by the credit card company.

In fraud detection, cluster analysis can be used to identify groups of customers or transactions with similar characteristics, such as the same source of funds, similar transaction patterns, or unusual behavior.

Decision Trees

Decision trees are a machine learning technique used to classify data points based on a set of rules. In fraud detection, decision trees can be used to classify transactions or customers as high-risk or low-risk based on specific criteria.

Neural Networks

Neural networks are a machine learning technique used to identify patterns in data. In fraud detection, neural networks can be used to identify unusual transaction patterns or high-risk customers.

Anomaly Detection

Anomaly detection is a statistical technique used to identify unusual patterns in data. In fraud detection, anomaly detection can be used to identify unusual transaction patterns or customer behavior. “Too good to be true” gives a very good clue in anomaly detection.

Clustering Algorithms

Clustering algorithms are a machine learning technique that groups’ data points together based on similar characteristics. In fraud detection, clustering algorithms can be used to identify groups of high-risk customers or transactions based on specific criteria.

Gaussian Mixture Models (GMM), K-means clustering etc. can be used for fraud detection with the help of software tools.

Overall, statistical and mathematical techniques play a crucial role in fraud detection techniques, as they enable financial institutions to analyse large volumes of data and detect potential fraud patterns. These techniques, when used in combination with other fraud detection methods, can help to prevent and detect fraudulent activities.

TECHNOLOGY BASED FRAUD DETECTION TECHNIQUES

There are several technology-based fraud detection techniques that organizations can use to prevent and detect fraud.

Here are some of the most common techniques used across the world with the help of fraud detection software programs to detect irregular patterns. This is because of enormous volume of data flowing into the business it will be impossible to unearth the fraud by manually going through thousands of transactions due to time and manpower constraints.

Data Analytics

Data analytics involves using algorithms and statistical models to analyze large amounts of data and identify patterns, anomalies, and outliers that may indicate fraud. With the help of data analysis software it is possible to search entire data files for red flags of possible fraud. The number of checkpoints a forensic auditor or forensic accountant can set-up using a data analysis software is very high.

Data analysis can help the forensic auditor in developing reference files for fraud detection. He can establish a norm to enable him to compare individual months or years.

Machine learning

Machine learning (ML) is a subset of Artificial Intelligence (AI), is a learning algorithm in a computer system that enables it to identify patterns and outliers in a large data.

ML has the ability to uncover hidden patterns and allows the forensic auditor the ability to derive meaningful information from the big data.

Machine learning involves using algorithms to analyse historical data and learn from it, so that the system can automatically detect and prevent fraud in real-time.

Machine learning algorithms can analyse large datasets to detect patterns and anomalies that indicate fraudulent behavior. These algorithms can be trained using historical data to identify suspicious transactions and behaviors.

This approach is especially useful in detecting credit card fraud, insurance frauds, where transactions can be analysed in real-time to identify suspicious activities.

It is humanly impossible to detect credit card frauds, insurance frauds etc., manually because of huge volume of data. Hence, Machine learning is extensively used.

1. **Fraud Detection Machine Learning Algorithms Using Logistic Regression**:

   Logistic Regression is a supervised learning technique that is used when the decision is categorical. It means that the result will be either 'fraud' or 'non-fraud' if a transaction occurs.

   Case:

   Let us consider a scenario where a transaction occurs and we need to check whether it is a 'fraudulent' or 'non-fraudulent' transaction. There will be given set of parameters that are checked and, on the basis of the probability calculated, we will get the output as 'fraud' or 'non-fraud.' If probability calculated is 0.9, this means that there is a 90 percent chance that the transaction is 'genuine' and there is a 10 percent probability that it is a 'fraud' transaction.

2. **Fraud Detection Machine Learning Algorithms Using Decision Tree**:

   Decision Tree algorithms in fraud detection are used where there is a need for the **classification** of unusual

activities in a transaction from an authorized user. These algorithms consist of constraints that are trained on the dataset for classifying fraud transactions.

Case:

Let us consider a scenario where a user makes some transactions. Forensic auditor will build a decision tree to predict the probability of fraud based on the transaction made. First, in the decision tree, Machine will check whether the amount is greater than ₹50,000? If answer is 'yes,' then it will check the I.P address location from where the transaction is made. And if it is 'no,' then it will check the frequency of the transaction.

After that, as per the probabilities calculated for these conditions, it will predict the transaction as 'fraudulent' or 'non-fraudulent.'

For instance, if the amount is greater than ₹50,000 and location is equal to the IP address of the customer, then there is only a 25% chance of 'fraud' and a 75% chance of 'non-fraud.'

Similarly, if the amount is greater than ₹50,000 and the number of locations is greater than 1, then there is a 75% chance of 'fraud' and a 25% chance of 'non-fraud.'

Thus a decision tree in Machine Learning helps in creating fraud detection algorithms.

3. **Fraud Detection Machine Learning Algorithms Using Neural Networks**:

Neural Networks is a concept inspired by the working of a human brain. Neural networks in Deep Learning uses different layers for computation.

Neural networks uses cognitive computing that helps in building machines capable of using self-learning algorithms that involve the use of data mining, pattern recognition, and natural language processing. It is trained on a dataset passing it through different layers several times.

It gives more accurate results than other models as it uses cognitive computing and it learns from the patterns of authorized behavior and thus distinguishes between 'fraud' and 'genuine' transactions.

Artificial Intelligence

Artificial intelligence refers to computer systems that are able to mimic human-like tasks like visual perception and decision-making. Examples of artificial intelligence that we use every day without even realising it are: Auto Pilot function in flights, spam filters in email and mapping apps in smartphones to analyse the traffic congestion and suggest the fastest route.

Artificial intelligence (AI) involves using machine learning algorithms and other advanced technologies to analyse data, detect patterns, and identify potential fraud.

Biometric Authentication

Biometric authentication involves using unique physical characteristics such as fingerprints, iris scans, or facial recognition to verify the identity of individuals and prevent fraud. This technology is increasingly being used in various industries to prevent identity fraud.

Behavior Analysis

Behavior analysis involves monitoring user behavior to identify patterns of behavior that may indicate fraudulent activity. This can involve analysing user login patterns, transaction histories, and other behavioral data. Behavioral analytics involves the analysis of user behavior to detect patterns that may indicate fraudulent activities. This technique is commonly used in the banking and finance industry to detect account takeover fraud, where a fraudster takes over an account and performs unauthorised transactions.

Real-time Transaction Monitoring

Real-time transaction monitoring involves using automated systems to monitor transactions as they occur, and flagging suspicious activity in real-time.

Digital Signature Verification

Digital signature verification involves using technology to verify the authenticity of digital signatures on documents and transactions, to prevent fraud.

Data mining techniques

These are used to analyse large amounts of data to identify hidden patterns and co-relationships that may indicate fraudulent activities. This approach is commonly used in the insurance industry to detect fraudulent claims. This can include analysing transaction histories, user behavior, and other relevant data points.

Digital identity verification

Digital identity verification techniques are used to verify the identity of individuals who are accessing online services or making online transactions. This approach is commonly used in the e-commerce industry to prevent fraudulent activities. One time passwords are sent to the user to his or her mobile to change password or even to do online transactions.

Blockchain Technology

Blockchain technology can be used to create secure and transparent records of transactions, making it more difficult for fraudsters to alter or manipulate data.

Two-Factor Authentication

Two-factor authentication requires users to provide two different types of authentication, such as a password and a one-time code sent to their phone, to access an account. This can help prevent unauthorised access and identity theft.

These are just a few examples of the many technology-based fraud detection techniques that organizations can use to prevent and detect fraud.

By leveraging advanced tools and techniques, businesses can better protect themselves and their customers from fraudulent activities.

DIGITAL FORENSICS TECHNIQUES

Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic data in a way that is admissible as evidence in a court of law. This includes retrieving data from computers, mobile devices, and other digital storage media to support legal cases.

Digital Evidence

In order to solve a cybercrime alleged to have been committed appropriate digital evidence have to be identified and collected, analysed and evaluated as to the suitability in the court of law and report have to be prepared by the digital forensic expert and submitted to those who have appointed him.

Fraud investigation will involve searching for and potential recovery of digital documents such as invoices, statements, order forms, spreadsheets and databases. Emails can also be a good source of information relating to fraud. It can contain information concerning contact between fraudsters, the passing of information such as credit card and bank account details.

The initial stage of dealing with the digital forensics aspect of a fraud detection investigation is capturing the data. Whether this is done by the police or by a forensic auditor on their behalf, the procedures are the same.

Information and evidence can be obtained from servers, workstations, laptops, removable storage media, mobile phones and other handheld devices of the entity. The collection of the data should be carried out by a trained and experienced person, in a manner which does not allow the original data to be altered in any way.

The process of capturing the data in such a secure manner is known as 'acquisition' or 'imaging'. It is achieved by capturing through a write protection device a very low level copy of the contents of the media. This, once processed, allows the investigator a view of the contents of the computer including those areas that would not normally be visible to a user. This is known as a forensic image.

The two tools most widely used for the processing and examination of a forensic image are 'EnCase' (produced by Guidance Software) and 'Forensic ToolKit' or 'FTK' (produced by AccessData). These allow the investigator to view the content of the images, conduct searches and potentially retrieve hidden and deleted data.

There are tools available which will attempt to recover items such as social networking chat logs and other artefacts, which may be missed. These items can be very helpful in a fraud detection investigation, as often, communication happens between culprits through instant messaging or 'Chat' on websites such as 'Facebook'.

Additionally, a record of Internet history can provide information that would be very useful to an investigator. For example, the fact that the Internet history on a suspect computer has entries of having visited various online banking websites, could indicate that a user with fraudulent intent has been visiting accounts of their targets. Mobile Forensics and Botnet Forensics are other important fraud detection techniques.

Digital forensics has been discussed at length in Chapter 14 Cyber Forensics

DATA MINING TECHNIQUES FOR FRAUD DETECTION

Data mining techniques have become increasingly important in fraud detection due to the sheer volume of data that needs to be processed and analysed in order to identify potentially fraudulent behavior. Employees using company credit cards for personal expenses, employees claiming reimbursement of expenses on a day they were not travelling are some examples.

Some common data mining techniques used in fraud detection are:

1. **Anomaly Detection:**

   This technique involves identifying data points that deviate significantly from the norm or expected patterns. This is called as outliers. In fraud detection, it can be used to identify transactions or behaviors that are unusual and may be indicative of fraud.

   For example regularly logging outside office hours and on holiday, or from a remote IP address are all anomalies which are used during investigation to detect manipulation of financial records and transactions fraudulently.

2. **Clustering:**

   This technique involves grouping similar data points together. In fraud detection, clustering can be used to group similar transactions or behaviors together, making it easier to identify patterns of fraudulent activity.

3. **Decision Trees:**

   Decision trees are graphical representations of decisions and their possible consequences. In fraud detection, decision trees can be used to create rules that identify potentially fraudulent behavior based on a series of criteria.

4. Neural Networks:

Neural networks are a type of machine learning algorithm that can learn from data and identify patterns. In fraud detection, neural networks can be used to identify complex patterns of fraudulent behavior that may not be immediately apparent.

5. Text Mining:

Text mining involves analysing unstructured text data, such as emails or chat logs. It is a method of using a specialised software to extract information from unstructured text data.

Through the application of linguistic technologies and statistical techniques, fraud keywords that are likely to point suspicious activity are mined from the texts.

Example of fraud keywords can be deadline, trouble, quota, short, concern, problem, override, write-off, adjust, reserve/provision, reasonable, deserve, temporary etc., are mined from the text by analysing the digital written communication or in the journal entries.

This list depend on the nature of industry, fraud scheme and the data set the forensic auditor. It also depends on whether they are searching emails or accounting records.

In the case of suspected bribery or corruption words in payment description can include consulting fees, goodwill payment, processing fee, donation, special commission, special payment, expediting fee, one-time payment and so forth.

In the text mining the emotional tone of the correspondence in emails and other digital messages, derogatory, surprised, secretive, worried and angry emotions communications can be used for detecting frauds.

In fraud detection, text mining can be used to identify suspicious language or topics that may be indicative of fraud.

6. Association Rules or Link Analysis:

Association rules are used to identify relationships between different variables. In fraud detection, association rules can be used to identify patterns of behavior that are commonly associated with fraudulent activity.

Data mining techniques can be very useful in identifying patterns of fraudulent behavior and detecting potential fraud. However, it is important to use these techniques in conjunction with other fraud detection methods, such as manual review and investigation, in order to ensure that accurate and actionable results are obtained.

WILFUL DEFAULTS AND EMERGING FORENSIC AUDIT ASPECTS UNDER INSOLVENCY AND BANKRUPTCY CODE, 2016

The term “wilful default” refers to a deliberate and intentional act of non-repayment of a loan or debt by a borrower despite having the ability and means to repay. It is a deliberate act of avoiding the payment. It is considered a serious offence under the Insolvency and Bankruptcy Code, 2016 (“IBC”). This is because it can result in significant financial losses for the lender and seriously impacts the financial system.

Under the IBC, a creditor can initiate insolvency proceedings against a borrower who has committed a wilful default. The creditor must first provide evidence to the insolvency resolution professional that the borrower has committed a wilful default. The insolvency resolution professional will then examine the evidence and determine whether the borrower has indeed committed a wilful default.

If the insolvency resolution professional finds that the borrower has committed a wilful default, the borrower may be barred from participating in the insolvency resolution process. The insolvency resolution professional may also recommend criminal proceedings against the borrower and its management for fraud or other offences.

"Wilful default" means "conscious and deliberate non-payment of dues by the corporate debtor despite having adequate means to pay, or the diversion of funds for purposes other than for which the loan was availed, or siphoning off funds so that it appears that the corporate debtor has become financially incapable of repaying the loan."

It is important to note that the determination of whether a borrower has committed a wilful -default is a fact-specific inquiry, and each case will depend on the particular circumstances involved. Factors that may be considered in making this determination include the borrower's financial condition, the borrower's ability to repay the loan, and the borrower's conduct in relation to the loan.

Under the Insolvency and Bankruptcy Code (IBC), wilful default is a serious offense, and the IBC provides for stringent penalties for defaulting borrowers who have acted willfully.

If a borrower is found to have acted willfully, the IBC empowers the creditor to initiate insolvency proceedings against the borrower. The wilful defaulter is not eligible for any concessions or exemptions, and the resolution process would be conducted without any moratorium or stay on legal proceedings. The wilful defaulter may also face criminal proceedings, which could result in imprisonment, fines, or both.

Emerging Forensic Audit Aspects under Insolvency and Bankruptcy Code, 2016

Forensic audit plays a crucial role in detecting and investigating frauds, irregularities, and non-compliances in insolvency and bankruptcy cases under the Insolvency and Bankruptcy Code, 2016 (IBC).

IBC is still a relatively new law, there are several emerging forensic audit aspects that are gaining importance in resolving insolvency and bankruptcy cases.

Some of these aspects are:

Pre-insolvency Forensic Audit:

Conducting a pre-insolvency forensic audit of the debtor's financial statements and records can help identify potential frauds, non-compliances, and irregularities that could impact the insolvency resolution process. This can help the resolution professional (RP) and the committee of creditors (CoC) in making informed decisions during the resolution process.

Investigation of Preferential Transactions:

Forensic audit can help investigate preferential transactions, which are transactions made by the debtor with related parties or other creditors to give them an unfair advantage over other creditors. Forensic audit can help identify such transactions and recommend actions to be taken to recover the assets involved.

Identification of Undisclosed Assets:

Forensic audit can help identify undisclosed assets of the debtor, which could be used to repay the creditors. This could include assets that were intentionally hidden by the debtor or those that were not disclosed due to negligence or oversight.

PUFE transactions by a debtor before the initiation of insolvency proceedings:

PUFE transactions refer to Preferential, Undervalued, Fraudulent, and/or Extortionate transactions that are made by a debtor before the initiation of insolvency proceedings under the Insolvency and Bankruptcy Code, 2016 (IBC) in India.

These transactions can significantly impact the insolvency resolution process, as they can reduce the assets available to repay the creditors.

Under the IBC, the resolution professional (RP) is required to examine all transactions made by the debtor during the relevant period to identify PUFE transactions. The relevant look back period is the period of two years preceding the insolvency commencement date.

If the RP identifies any PUFE transactions, they are required to make an application to the National Company Law Tribunal (NCLT) to declare such transactions as void. Once a transaction is declared void, the property or asset involved in the transaction is deemed to be vested with the debtor and becomes a part of the assets of the debtor's estate.

The IBC defines various types of PUFE transactions, as follows:

Preferential transactions: Section 43 of IBC

These are transactions made by the debtor to prefer one creditor over others. These transactions can be avoided if they were made within two years preceding the insolvency commencement date and the creditor had reasonable knowledge of the debtor's financial position.

IDBI Bank Ltd. v. *Jaypee Infratech Ltd.* **(***JIL***)** is a perfect example of transaction to be considered as preferential transaction.

The Allahabad Bench of the National Company Law Tribunal ("NCLT") observed that, the timing of entry of the transaction by JIL was questionable and JIL had entered into this transaction when it was facing severe financial difficulty". The Tribunal further observed that, the impugned transactions were entered into within the relevant period and are preferential transactions under Section 43 of the Code.

Undervalued transactions: Section 45 of IBC

These are transactions made by the debtor at a significantly lower value than the fair market value of the property or asset involved. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

Fraudulent transactions: Section 66 of IBC

These are transactions made by the debtor with an intention to defraud the creditors or any other person. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

The Supreme Court in (*M/s Embassy Property Developments* v. *State of Karnataka & Others*) laid down that NCLT and NCLAT have the jurisdiction to inquire into fraudulent transactions under section 66.

Extortionate transactions: Section 50 of IBC

These are transactions made by the debtor at an excessive price or amount in comparison to the prevailing market rates. These transactions can be avoided if they were made within two years preceding the insolvency commencement date.

Detection of Fraudulent Transactions:

Forensic audit is involved when there several entities / huge transactions involved, showing assets stripping/ funds diversions / Round tripping and fraud observed; Forensic Audit – runs beyond 2 years.

Forensic audit can help detect fraudulent transactions made by the debtor, including those made to siphon off funds, inflate revenues or assets, or misrepresent financial statements. Such transactions can be investigated and reported to the Committee of Creditors and the National Company Law Tribunal (NCLT).

Investigation of potential wrongdoing by promoters:

Forensic audit can also help investigate potential wrongdoing by the promoters of the debtor company, including mismanagement, diversion of funds, and other fraudulent activities that could have led to the insolvency or bankruptcy of the company.

CASE LAWS

Case laws on IBC, 2016

National Company Law Appellate Tribunal - *M. Srinivas vs. Ramanathan Bhuvaneshwari*

Resolution Professional filed application under section 66 of IBC for recovery of Rs. 46 crore, being receivables, inventory and P & M diverted; Adjudicating Authority ordered directed Central Government to initiate investigation by SERIOUS FRAUD INVESTIGATION OFFICE (SFIO) ; Now Ministry of Corporate Affairs investigation is on, based on National Company Law Appellate Tribunal (NCLAT) orders, modifying order of Adjudicating Authority.

National Company Law Tribunal (Mumbai) - *Rama Ratan Kanoongo vs. Sunil Kathuria*

Resolution Professional (RP) filed application for Liquidation of Corporate Debtor (CD); RP also sought for recovery of Rs.135 Lakhs being preferential transaction with one of the respondents;

NCLT Mumbai observed that this transaction was not done in the ordinary course of business of CD, as stock has been transferred and no payment has been made for the same; The transaction is satisfying the criteria of Section 43 of the Code and is to be labelled as preferential transaction and the prayers of the Applicant are allowed.

Adjudicating Authority also ruled that the treatment of avoidance or preferential or undervalued transaction is applicable even at the stage of liquidation.

LESSON ROUND-UP

- **Fraud:** Wrongful or criminal deception intended to result in financial or personal gain.
- **Investigation:** The action of investigating something or someone; formal or systematic examination or research.
- **Detection:** The action or process of identifying the presence of something concealed.
- **Fraud detection** is the process of identifying and preventing fraudulent activity in various contexts, including financial transactions, online interactions, insurance claims, and more. It is an important tool for individuals and organizations to protect themselves against financial losses and reputational damage caused by fraud. It is a postmortem after the alleged fraud has happened and a reactive action.
- **Early warning indicators of Fraud** such as Unusual Financial Activity, Poor Accounting, Unusual behavior, Unexplained Inventory, Employee Turnover, Weak or lack of Internal Controls, Complaints or Tip, Weaknesses in IT Security, Suspicious Emails or Messages
- **Money laundering** starts with proceeds from a specific source. For a variety of reasons the launderer wants to hide the money trail. Money laundering takes place in three distinct stages: Placement, Layering and Integration. The money launderers including drug dealers, fraudsters, tax evaders and terrorists have many challenges when moving money through each of the stage.

- The responsibilities of the external auditor as they relate to fraud detection are clearly defined in International Standard on Auditing (ISA-240), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.

  "The auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud. The requirements in this are designed to assist the auditor in identifying and assessing the risks of material misstatement due to fraud and in designing procedures to detect such misstatement"

- **Statistical and mathematical techniques** play a crucial role in fraud detection techniques, as they enable financial institutions to identify and analyze large volumes of data to detect potential fraud patterns.
- **Benford's Law** is a statistical tool used to detect potential fraud in financial statements or other numerical datasets. The law states that in many naturally occurring datasets, the leading digit is more likely to be a small number (e.g., 1, 2, or 3) than a large number (e.g., 8 or 9). One application of Benford's Law is in detecting fraudulent journal entries or fraudulent financial transactions in the books of account.
- **Regression Analysis** is a statistical technique that examines the relationship between two or more variables. In fraud detection, regression analysis can be used to identify relationships between variables, such as the correlation between high-risk customers and suspicious transactions.
- **Cluster Analysis:** Cluster analysis is a statistical technique that groups similar data points together.
- The term **"wilful default"** refers to a deliberate and intentional act of non-repayment of a loan or debt by a borrower despite having the ability and means to repay. It is a deliberate act of avoiding the payment. It is considered a serious offence under the Insolvency and Bankruptcy Code, 2016 ("IBC"). This is because it can result in significant financial losses for the lender and seriously impacts the financial system.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

Multiple Choice Questions (MCQs)

1. Act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity is called

   A. email bombing

   B. Spamming

   C. Cyber stalking

   D. Phishing

2. An activity that uses accounting, auditing and investigative skills to assist in legal matters, is known as:
    A. Fraud Audit
    B. System Audit
    C. Forensic Audit
    D. Due Diligence
3. Application of accounting methods to the tracking and collection of forensic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud, is known as:
    A. Forensic Accounting
    B. Forensic Audit
    C. Forensic Investigation
    D. None of the above
4. Know your Customer (KYC) regulations have been introduced in financial transactions under which of the following Act?
    A. Prevention of Money Laundering Act
    B. Companies Act
    C. Reserve Bank of India Act
    D. Banking Regulations Act
5. Which are the following steps in Money Laundering: Placement, Layering, Integration and Counterfeiting
    A. Only 2 and 4
    B. 1, 2 and 4
    C. 1, 2 and 3
    D. 1, 2, 3 and 4

Answer: (1) D (2) C (3) A (4) A (5) C

Practice Questions

1. What are the early warning indicators of fraud to be kept in mind by a forensic auditor?
2. Explain some of the common techniques used for fraud detection in money laundering.
3. Explain how Benford's law can be used a tool in fraud detection technique.
4. Explain the Data Mining techniques adopted by forensic auditors in Fraud Detection.
5. Explain the Statistical and Mathematical Techniques adopted by forensic auditors in Fraud Detection.
6. Discuss in detail emerging forensic audit aspects under Insolvency and Bankruptcy Code, 2016.
7. Explain the terms PUFE under the IBC, 2016 with examples.

LIST OF FURTHER READINGS

- **Forensic Audit Decoded**

  Author: G.C. Pipara

  Publishers: Taxmann

- **Forensic Audit**

  Author: CA Kamal Garg

  Publishers: Bharat's

WARNING

Regulation 27 of the Company Secretaries Regulations, 1982

In the event of any misconduct by a registered student or a candidate enrolled for any examination conducted by the Institute, the Council or any Committee formed by the Council in this regard, may suo-moto or on receipt of a complaint, if it is satisfied that, the misconduct is proved after such investigation as it may deem necessary and after giving such student or candidate an opportunity of being heard, suspend or debar him from appearing in any one or more examinations, cancel his examination result, or registration as a student, or debar him from re-registration as a student, or take such action as may be deemed fit.

It may be noted that according to regulation 2(ia) of the Company Secretaries Regulations, 1982, 'misconduct' in relation to a registered student or a candidate enrolled for any examination conducted by the Institute means behaviour in disorderly manner in relation to the Institute or in or around an examination centre or premises, or breach of any provision of the Act, rule, regulation, notification, condition, guideline, direction, advisory, circular of the Institute, or adoption of malpractices with regard to postal or oral tuition or resorting to or attempting to resort to unfair means in connection with writing of any examination conducted by the Institute, or tampering with the Institute's record or database, writing or sharing information about the Institute on public forums, social networking or any print or electronic media which is defamatory or any other act which may harm, damage, hamper or challenge the secrecy, decorum or sanctity of examination or training or any policy of the Institute.

PROFESSIONAL PROGRAMME
INTERNAL & FORENSIC AUDIT
GROUP 1 • ELECTIVE PAPER 4.2

(*This test paper is for practice and self-study only and not to be sent to the Institute*)

Time allowed: 3 hours *Maximum Mark: 100*

Answer all Questions

PART I - INTERNAL AUDIT (60 MARKS)

Question No. 1

(a) ABC Ltd. (major player in automobile industry) appoints M/s Sahni and Co. to conduct an Internal Audit. Mr. A, an article assistant in M/s Sahni and Co., while conducting an internal audit undertake informal oral inquiries with staff of ABC Ltd. During this process, one of the staff member of ABC Ltd. revels to Mr. A about a cash related fraud committed by cashier. In order to go deep to reveals about the fraud, Mr. A had a discussion with senior officer in Accounts department and concluded that cash related fraud has been committed by cashier. Mr. A asked for the written confirmation from the staff and officers in the accounts department but both had refused to give any written confirmation and denied that fraud have been committed.

What will be the next course of action by Mr. A as an Internal Auditor?

(b) Aruna Ltd, a listed company, headquartered in Mumbai, Maharashtra has appointed M/s Rao and Co (Practicing Company Secretaries) to conduct an internal audit of the company. The internal auditor, during the review of tax liabilities of GST with respect to goods and services provided during the period under audit, reveals that a total of around 1000 transactions (valued around Rs. 1500 crore) goods and services have been provided wherein incorrect GST rates were applied (9% has been charged instead of 18%) resulting into excess GST liability of Rs. 46 crore.

In this situation, what should be the next course of action of the Internal Auditor?

(c) Moon Limited, a listed company, headquartered in delhi, is in the business of providing hi-tech consulting services in India as well as globally. It has around 135 client base in India and around 45 clients outside India to whom it provides hi-tech consulting services inclusion technology based solution.

Moon ltd. has around 1000 employees and having in house Internal Audit Department. Further, it appoints Mr. Sujan and Co. (Practicing Company Secretary) for conducting internal audit. During the period under review, the internal auditor (Mr. Sujan) observed that there are few employees to whom appointment letter has not been issued and further there are no mechanism to capture in and out time of those employees.

This matter has been brought to the notice of the management by the internal auditor. Management stated that these employees are trainee for 2-3 months and therefore appointment letter has not been issued to them. Further, very small amount is paid as stipend and therefore, in-time and out-time of the trainees are not captured.

In this situation, what should be the next course of action of the Internal Auditor?

(d) While conducting the Internal Audit of the Company, the internal auditor has observed the following while reviewing the employees official travelling expenses:

i. Not able to trace the request and approval for travelling. Also, the travelling record does not reveals the reason of travel.

ii. Employees mostly travelled by their own vehicle and claimed reimbursement on the basis of kilometer travelled. No other supporting documents were attached to substantiate the travel actually performed.

iii. In case of travels performed by Air where boarding passes were missing as a proof of travel.

In this situation, what action should be taken by the Internal Auditor?

(5 Marks each)

Question No. 2

(a) A firm comprising of two partners who take active part in running the vegetable business, with two assistants. The firm has simple accounting system and does not need more than a cash and bank book to record. Expenses such as rent and insurance, Purchase of vegetables like cabbages, carrot, potatoes, onion etc. Sale of vegetables etc.

The expenses and purchases are supported by two box files of "paid" and "unpaid invoices" and they have billing machine to record sales.

As an internal auditor how would you ensure that sales and purchases were completely and accurately recorded?

(b) The office manager controlled the company's financial operations. She did payroll, accounts payable, invoicing and cash receipts. She rarely took time off, and even then, came back when they needed to run checks or payroll. The owner viewed her as key to running the business. What are your recommendations as an internal auditor of the organizations in view of evaluating Internal Control Mechanism?

(c) ABC Pvt. Ltd. having Rs. 90 lacs paid-up capital, Rs. 5 crores reserves and turnover of last three consecutive financial years, immediately preceding the financial year under audit, being Rs. 50 crores, Rs. 175 crores and Rs. 300 crores, but does not have any internal audit system. In view of the management, the internal audit system is not mandatory. Comment?

(d) Mr. ABC is the chief Internal Auditor of M/s XYZ Pharmaceuticals Private Limited. The company has spread its sales operations across 20 countries through Distributors and Dealers network. For the purpose of local connections and compliances, the Company has opened branch offices in each country. Apart from this, the Company has manufacturing facilities in India and China. For the purpose of manufacturing raw material, technology is imported from various countries including USA, France and Japan. The key statistics of the company are mentioned below:

1. Annual Turnover of the Company – Rs. 25,000 crores approx.
2. Total Manpower – 8000 employees
3. Total Branches – 18

Audit Committee has asked Chief Internal Auditor (CIA) to prepare audit plan for 3 years. Please suggest the steps to be followed by the CIA and prepare audit universe of the Company.

(5 Marks each)

Questions No. 3

(a) XYZ advisors is a management consulting firm having 250 fortune company client base. The CEO of the company is concerned about high employee attrition rate in his company. He has given assignment to dig out the reason for such high attrition rate as well as way forward. What factors would an Internal Auditor consider while conducting such analysis?

(b) Internal auditor carried out a physical verification of Fixed Deposit Receipts on a surprise basis and tallied it with the Ledger balance. Finding no discrepancy the auditor submitted an assurance report. Finance head expressed the view that since this exercise was always carried out by the statutory auditors at the end of the year, this was a redundant exercise.

What should be the response of Internal Auditor in this situation?

(c) State with reasons (in short) whether the following statements are correct or incorrect:

i. "Audit Documentation", the working papers are not the property of the auditor.

ii. Purchase invoice is an example of internal evidence.

iii. Sufficiency is the measure of the quality of audit evidence.

iv. Inquiry alone is sufficient to test the operating effectiveness of controls.

v. Universe refers to the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions.

(d) The paid-up share capital X Private Ltd. as on 31.03.2022 is Rs. 1.50 crores. The reserves and surplus as on that date is Rs. 30 lakhs. The turnover of X Private Ltd as per Profit and loss account for financial years 2019-20, 2020-21 and 2021-22 are as follows:

Financial Year	*Turnover (Rs. in crores)*
2018-19	7
2019-20	12
2020-21	15

Will the company be exempt from CARO, 2020 for the financial year 2021-22?

(5 Marks each)

PART II – FORENSIC AUDIT (40 MARKS)

Question No. 4

Shree Capital, a 'NBFC', registered and having banking license to operate, perform and channelize the banking operation in the district of Kolhapur (Maharashtra). The banks headquarter is situated at Kolhapur and having 12 branches situated at various remote locations in the district of Kolhapur.

Objectives: The main objects of the Shree Capital is to provide crop agriculture loans (grapes loan) to the farmers (who involved in producing the grapes) in remote location in the district of Kolhapur. The loan granted to the farmers were without any collateral security and therefore categorized as personal loan.

Financial Performance: The Financial Statement of the Shree Capital showing the net profit (increasing trends) for last 4-5 years and reflecting Non-Performing Assets 'NPA' less than 0.5% in previous years .

On the other hand, the farmer's wealth conditions in the district of Kolhapur got worse during the last 4-5 years, due to crop destroyed on account of bad weather conditions.

Preliminary Investigation: Based on preliminary investigation, the following facts are revealed:

i. The Kolhapur districts have two sugar factories. The local farmers also worked (part time) in these factories to earn their livelihood.

ii. The financial condition of sugar factories are not good for last 4-5 years and the local banks have refused to provide loan assistance to the sugar factories.

iii. Despite of financial crisis, the sugar factories smoothly carried out the production process.

iv. Banks senior employees have good connect with the management team of the sugar factories.

v. In the books of account of the banks, all the 12 EMI's for the year (with respect to loan granted to farmers) were collected on the last day of the previous year and not on monthly basis.

vi. The personal wealth of the senior employees of the bank was increased 4 times in past 4-5 years.

vii. The bank's documentation regarding the loan requisition form, sign etc. were properly maintained.

On the basis of the above, draw up a plan of action which you will adopt to fulfill your work to (suitable assumption may be made by you) indicate your approach in the following areas:

(a) Detailed Methodology.

(b) Findings of the case based on your methodology.

(c) Limitations of the forensic report.

(d) Legal steps that could be taken against NBFC, its subsidiaries and their directors.

(5 Marks each)

Question No. 5

(a) Mr. X received an email from the Income Tax Dept., mentioning the following :

> Dear Taxpayer,
>
> You have filed your income tax return for the Assessment Year 2023-24 and a refund of Rs. 14,600 is payable to you. However, the account mentioned by you is incorrect and requires validation.
>
> Please visit the following link in order to validate your account.
>
> *http:/jncometaxindiafiling.jov.com*
>
> Note: Failure to validate your account number will lead to rejection of refund.
>
> *Regards Team* : Income Tax Department
>
> Pay tax honestly and contribute in Nation's Development

What Mr. X should do in the mentioned situation?

(10 Marks)

(b) Arjun Ltd. is a registered supplier of spare parts of spinning mills and covered under the GST law. Their turnover for the year ended 31st March, 2022 is Rs. 800 crores and they have filed their return of income on 6th September, 2022.

Arjun Ltd. borrowed a working capital (cash credit limit) from a bank of Rs. 150 Crore. Arjun Ltd. regularly submit the month end closing stock statements of each month to bank without delay.

A bank suspects that the stock statements furnished by Arjun Ltd for the last 12 months do not reflect the true position and that they have been systematically furnishing statements showing higher quantities of various items of stock as compared to the actual quantity present in their godowns, and also that the values have been overstated.

The bank has appointed you as the forensic auditor. Explain, how will you go about gathering evidence and what are the documents, statements, returns, etc., you will go through to check the veracity of the stock statements furnished by the borrower?

(10 Marks)

****

To join Classes, please go through the contact details of Regional/Chapter Offices of the Institute of Company Secretaries of India as per details mentioned below

EASTERN INDIA REGIONAL OFFICE (KOLKATA): 033-22901065, eiro@icsi.edu

- Bhubaneswar: 0674-2552282; bhubaneswar@icsi.edu
- Dhanbad: 0326-6556005; dhanbad@icsi.edu
- Guwahati (NE): 0361-2467644; guwahati@icsi.edu
- Hooghly: 033-26720315; hooghly@icsi.edu
- Jamshedpur: 0657-2234273; jamshedpur@icsi.edu
- Patna: 0612-2322405; patna@icsi.edu
- Ranchi: 0651-2223382; ranchi@icsi.edu
- Siliguri: 0353-2432780; siliguri@icsi.edu

NORTHERN INDIA REGIONAL OFFICE (NEW DELHI): 011-49343000, niro@icsi.edu

- Agra: 0562-4031444; agra@icsi.edu
- Ajmer: 0145-2425013; ajmer@icsi.edu
- Alwar: 0144-2730446; alwar@icsi.edu
- Amritsar: 0183-5005757; amritsar@icsi.edu
- Bareilly - 0581-4050776; bareilly@icsi.edu
- Bhilwara: 01482-267400; bhilwara@icsi.edu
- Bikaner: 0151-2222050; bikaner@icsi.edu
- Chandigarh: 0172-2661840; chandigarh@icsi.edu
- Dehradun: 8266045008; dehradun@icsi.edu
- Faridabad: 0129-4003761; faridabad@icsi.edu
- Ghaziabad: 0120-4559681; ghaziabad@icsi.edu
- Gorakhpur: 0551-3562913; gorakhpur@icsi.edu
- Gurugram: 0124-4232148; gurugram@icsi.edu
- Jaipur: 0141-2707236; jaipur@icsi.edu;
- Jalandhar: 0181-7961687; jalandhar@icsi.edu
- Jammu: 0191-2439242; jammu@icsi.edu
- Jodhpur: 0291-2656146; jodhpur@icsi.edu
- Kanpur: 0512-2296535; kanpur@icsi.edu
- Karnal: 9877938334; karnal@icsi.edu
- Kota: 0744-2406456; kota@icsi.edu
- Lucknow: 0522-4109382; lucknow@icsi.edu
- Ludhiana: 0161-2401040; ludhiana@icsi.edu
- Meerut: 0120-4300148; meerut@icsi.edu
- Modinagar: 01232-298162; modinagar@icsi.edu
- Noida: 0120-4522058; noida@icsi.edu
- Panipat: 0180-4009144; panipat@icsi.edu
- Patiala: 9812573452; patiala@icsi.edu
- Prayagraj: 0532-4006166; prayagraj@icsi.edu
- Shimla: 0177-2672470; shimla@icsi.edu;
- Srinagar: 0194-2488700; srinagar@icsi.edu
- Udaipur: 88520 85020; udaipur@icsi.edu
- Varanasi: 0542-2500199; varanasi@icsi.edu

SOUTHERN INDIA REGIONAL OFFICE (CHENNAI): 044-28222212, siro@icsi.edu

- Amaravati: 0863-2233445; amaravati@icsi.edu
- Belagavi: 0831-4201716; belagavi@icsi.edu
- Bengaluru: 080-23111861; bengaluru@icsi.edu;
- Coimbatore: 0422-2237006; coimbatore@icsi.edu
- Hyderabad: 040-27177721; hyderabad@icsi.edu
- Kochi: 0484-2375950; kochi@icsi.edu
- Kozhikode: 0495-2770702; calicut@icsi.edu
- Madurai: 0452-4295169; madurai@icsi.edu
- Mangaluru: 0824-2216482; mangalore@icsi.edu
- Mysuru: 0821-2516065; mysuru@icsi.edu
- Palakkad: 0491-2528558; palakkad@icsi.edu
- Salem: 0427 - 2443600; salem@icsi.edu
- Thiruvananthapuram: 0471-2309915; tvm@icsi.edu
- Thrissur: 0487-2327860; thrissur@icsi.edu
- Visakhapatnam: 0891-2533516; vpatnam@icsi.edu

WESTERN INDIA REGIONAL OFFICE (MUMBAI): 022-61307900, wiro@icsi.edu

- Ahmedabad: 079-26575335; ahmedabad@icsi.edu;
- Aurangabad: 0240-2451124; aurangabad@icsi.edu
- Bhayander: 022-28183888; bhayander@icsi.edu
- Bhopal: 0755- 2577139/4907577; bhopal@icsi.edu
- Dombivli: 0251-2445423; dombivli@icsi.edu
- Goa: 0832-2435033; goa@icsi.edu
- Indore: 0731-4248181; indore@icsi.edu
- Kolhapur: 0231-2526160; kolhapur@icsi.edu
- Nagpur: 0712-2453276; nagpur@icsi.edu
- Nashik: 0253-2318783; nashik@icsi.edu
- Navi Mumbai: 022-49727816; navimumbai@icsi.edu
- Pune: 020-25393227; pune@icsi.edu
- Raipur: 0771-2582618; raipur@icsi.edu
- Rajkot: 0281-2482489; rajkot@icsi.edu
- Surat: 0261-2463404; surat@icsi.edu
- Thane: 022-46078402; thane@icsi.edu
- Vadodara: 0265-2331498; vadodara@icsi.edu

CCGRT, NAVI MUMBAI : 022-41021503 - CCGRT, HYDERABAD : 040-23399541

Connect with ICSI www.icsi.edu | | Online Helpdesk : http://support.icsi.edu